Item 11
For Noting

Glasgow Kelvin College

Audit and Risk Committee Meeting of 22 February 2022

Risk Management Update

Report by Vice Principal Operations and Director Of Corporate Services

1. Introduction

It is normal practice that the Strategic Risk Register is considered at every meeting of the Audit and Risk Committee, Risk Management Committee and is considered twice per year by the Board of Management and once per year by each of the other formal Sub Committees of the Board.

A copy of the Strategic Risk Register as at 15 February 2022 is provided for information at **Appendix 1.**

2. Risk Management Activities

Since the last Audit and Risk Committee in November 2021 and Board Meeting in December 2021, a number of activities have taken place in relation to Risk Management:

- The membership of the College's Risk Management Committee has been updated to reflect the new Terms of Reference approved in December 2021;
- The Risk Management Teams site has been redeveloped to create space for the new Team Risk Registers so that these are held and maintained in once location. Access is appropriately managed;
- All staff Risk Management Awareness Sessions took place on Tuesday, 18 January 2022 at 10am and on 24 January 2022 at 4pm. These sessions, which were optional for staff, were delivered by Alan Ross from Zurich and well over 100 people attended. The second one was recorded and slides were made available. This will be uploaded to the College staff area and promoted again over the next quarter;
- The College's Risk Management Committee met on 25 January 2022; and
- A further Team Risk Register will be created for Communications and Marketing given the focus on this area moving forward. The session to create the Register, again facilitated by Zurich, is scheduled for 23 February 2022.

3. Risk Register Review

The new Strategic Risk Register has been in place since December 2021. At the Board of Management meeting on 13 December 2021, it was agreed that a new risk would be added to specifically cover the ongoing implications of Covid 19. This Register was presented to the College's Risk Management Committee on 25 January 2022 and no changes were made at this time.

The Risk Title, Residual Risk Score and colour of the twelve risks which could impact on the College's ability to deliver its strategic ambitions are summarised in the table below including Inherent Risks Scores/Categories and Residual Risks Scores/Categories. The scores are unchanged since the last Board Meeting - full detail is at **Appendix 1**.

Risk Ref No	Date Identified	Risk Title	IR	IR	RR	RR	Risk Appetite Category	Movement in Period
1	04/11/2021	SFC Review	20	**Very High**	12	**High**	1. Policy	↔
2	04/11/2021	GKC Identity	16	**Very High**	9	**High**	2. Reputation	↔
3	04/11/2021	People	20	**Very High**	4	**Medium**	5. Workforce	↔
4	04/11/2021	Litigation / Compliance	16	**Very High**	3	**Medium**	7. Legal & Compliance (including Health	↔
5	04/11/2021	Curriculum Relevance	16	**Very High**	9	**High**	6. Student Experience	↔
6	04/11/2021	Sustainable Funding	16	**Very High**	12	**High**	3. Financial	↔
7	04/11/2021	Student Experience	16	**Very High**	9	**High**	6. Student Experience	↔
8	04/11/2021	Environment	16	**Very High**	9	**High**	8. Environmental Sustainability	↔
9	04/11/2021	Digital Transformation	16	**Very High**	6	**Medium**	4. Digital	↔
10	04/11/2021	Student Recruitment & Retention	20	**Very High**	12	**High**	6. Student Experience	↔
11	04/11/2021	Cyber Risk	25	**Very High**	12	**High**	2. Reputation	↔
12	13/12/2022	COVID-19 - Ongoing Implications	25	**Very High**	12	**High**	1. Policy	↔

The College considers risks on an ongoing basis these include:

- Covid-19 and related negative effects on credits/delivery/students/staffing/resources.
- An emerging/changed world/hybrid learning and teaching/working/the job market.
- Brexit and related negative effects on staffing and supplies i.e. shortages.
- The impacts of the Climate Emergency.
- The Review of Coherent Provision and Sustainability of the Glasgow Region.
- Inflation/cost of living, high energy and food prices.
- National Insurance increases (April 2022).
- Mental health/delays to operations etc.
- NJNC – Formal Notification of Dispute.
- Budget Cuts for 2022-23.
- SFC – In Year Redistribution of Credit Activity for AY 2021-22.
- Foundation Apprenticeship delivery.

Further information/detail has been provided on some of the above items throughout this report.

4. NJNC – Formal Notification of Dispute

Audit and Risk members have been provided with a copy of the correspondence received under agenda Item 16.

There is a real risk of industrial action as a result of this pay dispute. The actual dispute is managed nationally and is not technically within the College's gift to resolve. However, the College has had previous experience of managing and mitigating the impact of such action, but

this would be particularly challenging given the impact on learning and teaching already experienced this year.

5. Budget Cuts for 2022/23

Audit and Risk members have been provided with a copy of the correspondence received under agenda Item 17.

Current indications are that, while the College was very prudent in setting its three year budgets, there is a significant negative budget implication for 2022/23 and beyond, specifically in relation to Foundation Apprenticeship income. SFC still requires to provide clarification in relation to certain aspects of this. Until this is received, it will be impossible to determine the full impact on the College's financial position for next year.

This funding allocation will also impact on how the College manages the changes required at Section 6 below.

6. SFC – In Year Redistribution of Credit Activity for AY 2021-22

Audit and Risk members have been provided with a copy of the correspondence received under agenda Item 18.

SFC has notified Colleges of its intention to clawback funding this year for undelivered Credits; while this is normal practice, it has not happened in the previous two Academic Years since the pandemic hit and was not expected this year. The College has provided an anticipated number to the SFC and it is expected that, in the first instance, Credits will be reallocated across the Glasgow Region.

The maximum value that will be clawed-back is 75% of the Credit Value and this will be factored in to the Quarter 2 Financial Forecast.

7. Foundation Apprenticeship Delivery

Following months of discussion, a decision has been taken to disband the Regional Foundation Apprenticeship Team, which is managed by the College. The three individual Colleges will manage and deliver their own Foundation Apprenticeships (FAs), but a regional steering group will maintain regional coordination of programmes offered by the three colleges. This will also provide a forum to promote collaborative approaches, ensure that class sizes are viable and minimise any unintended competition. Recruitment for 2022/23 is still being led by the Regional Team but, from next year, the plan is to have a digital front door for Glasgow for the FA programme.

An Executive Committee meeting was held on Thursday, 10 February 2022 to discuss this in detail and the FA Team was told of the plans on the morning of Friday, 11 February 2022.

The paper presented to the Executive Committee highlights a number of risks and mitigating actions in relation to managing this change.

8. Air Handling Unit Installation

The College began work on the replacement of the main air-handling units at its Springburn Campus building on Thursday, 10 February 2022. While units at all other campuses are still relatively new in terms of their service lifespan, the existing air-handling units at Springburn are over 12 years old and, as part of the estates capital plan, required to be replaced. This project has cost over £310k and is nearing completion.

The aim of the replacement of the units is to future-proof the College with energy-efficient air-handling units that are fit-for-purpose, economical and deliver significant improvements in air quality at Springburn Campus, while maintaining the College's commitment to sustainability and the environment.

The new units will be able to process a greater cubic volume of air compared to the previous units, while new filtration racks will greatly improve the air-quality throughout the building benefitting staff, students and visitors.

The works will represent an overall cost saving to the College through significant improvements in energy efficiency resulting in reduced energy bills and a further reduction in the College's carbon footprint.

Images of the works to replace the air-handling units are attached as **Appendix 2** to the report. This project was a massive undertaking involving late night and weekend working for minimal disruption to College operations.

9. Fire Risk Assessment

An annual fire risk assessment was carried out at all campuses. At the time of writing this report, the final report is awaited. Minor issues were flagged and these are being worked on at present whilst we await the report.

The final report and all actions taken will be communicated to Audit and Risk members.

10. Cladding

During a period of extremely windy weather, a very small cladding panel was dislodged from the Springburn Campus building and fell to the ground. This was obviously very unexpected and should not have happened. Checks have been made of the cladding panels in previous years and minor repairs were made. For completeness, a full review of all cladding panels has been undertaken and any work required will be carried out as a matter of urgency.

Due to Brexit, purchasing replacement panels from suppliers in the EU is proving problematic.

11. Vandalism at East End Campus

During the pandemic, it has become apparent that teenage gangs are beginning to form; this is likely to be in relation to youth centres, clubs, sports facilities etc being closed. The press story is at the link below:

Scotland Racing Headlong into a Teen Gang Crisis

It was with sadness that we noted our recycling bins in our new East End Community Garden were destroyed by fire over one weekend in an act of vandalism.

We are keen that no further damage to our Community Garden occurs and that this area is retained as a welcome sanctuary/learning opportunity for the students, staff and communities of the College. As such, we have felt it necessary to have the Garden monitored/patrolled by one of our Security companies for a trial period of time.

A temporary security tower has been installed which is a mobile camera unit and works as a perimeter alarm system. This is monitored by a monitoring station which enables an operator to speak directly to people, who may intend to vandalise the garden, that the Police have been contacted. Images relating to this matter are shown at **Appendix 3**.

12. High Energy Prices

Members will be aware of the global trend in significant increases in energy prices. Gas and electricity prices continue to increase across short-term and long-term contracts. Compared with the last Price Risk Guidance, there has been a consistent upward price movement which showed little sign of easing moving from 2021 into 2022.

How has the gas & electricity price position changed?

- Future seasonal gas prices increased by between 21% and 73% from Oct to Dec 2021
- Future seasonal electricity prices increased by between 17% and 59% from Oct to Dec 2021
- Upward price movement across all seasons has averaged 36% for gas and 31% for electricity
- 83% of gas and 86% of electricity requirements for 2022/23 are already purchased.

What has been driving prices?

- Russia and their increasing threat to invade Ukraine.
- Nord Stream 2 gas pipeline to Germany remains a political pawn. The US has reiterated its threat to block the pipeline should Russia invade Ukraine.
- European gas storage withdrawals are a concern, as levels reduce to 62% (Dec 21).
- Omicron impact is being monitored, what future restrictions may look like and how this could influence energy costs.
- Asian demand for Liquified Natural Gas (LNG) remains moderate, as UK imports increase.
- Colder weather temperatures and low wind (reducing wind turbine energy generation) are current key energy cost drivers.

Wider market positions

- Oil has marginally decreased to $73/barrel
- EU Carbon had strengthened to €84, but since decreased to €73
- UK Carbon had also strengthened to €79 and moved down to €76
- Sterling has seen a slight decline to 1.17 £/€ and 1.32 £/$
-

Estimated wholesale costs, if the College purchased all energy today (based on recent estimates):

Gas	Estimated Wholesale Cost @ 20/12/21	Electricity	Estimated Wholesale Cost @ 20/12/21
Apr22-Mar23	**2.620p/pkWh** (83% of volume already purchased)	Apr22-Mar23	**7.231p/pkWh** (86% of volume already purchased)
Apr23-Mar24	**2.513p/pkWh** (50% of volume already purchased)	Apr23-Mar24	**7.989p/pkWh** (50% of volume already purchased)

What measures are in place to mitigate price volatility and exposure to customers?

- Scottish Procurement Alliance have a Risk Management Committee who oversee policy, procedures and the performance of the purchasing strategy.
- Regular reports are provided on market conditions, future energy purchases already secured, exposure to risk and can take mitigating action when necessary, to protect the strategy.
- Scottish Procurement Alliance purchase gas and electricity up to 2½ years in advance, which has provided a high level of protection from the current record high prices. It also means 83-86% of next year's energy has already been purchased and 50% for 2023/24.
- By purchasing over a long period of time, it smooths out the volatility of energy prices and provides customers with a secure and fixed price each year.

- Scottish Procurements due diligence means there is no security of supply concerns for Natural Gas or Electricity. Our Suppliers are stable and not exposed the financial pressures which have seen smaller energy firms collapse.

The effect of the massive increase in energy prices will negatively affect our students, staff, suppliers etc.

13. Mental Health

Negative impacts of the pandemic are particularly prevalent in relation to poor mental health and has resulted in higher course drop-out rates. For students' personal and citizenship development, they require the opportunity to see each other in person and make connections; this has not occurred due to home learning.

The College is aware of the challenges that many students, and indeed staff, will face as we return to in-person teaching/learning and working. Many people will have undertaken only limited amounts of on-campus activity during the past two years and it is likely that a large number of people will be apprehensive, particularly those who are clinically vulnerable or are in close contact with others such as family members who are clinically vulnerable. It is therefore important that consideration is given to how this transition back to greater in-person teaching/learning/working will be managed, and what level of support will be required to ensure that all staff, students/learners' needs will be met.

The College is employing a Wellbeing and Engagement Lead to assist with addressing poor mental health.

14. Governance Questions Still to be Answered

The article attached Appendix 4 - Article , suggests that there is a concern in relation to governance arrangements within Scotland's colleges and discusses the Board of Management of Glasgow Clyde College being removed in 2015 and the current situation unfolding at South Lanarkshire College.

As has been evident previously, it is likely that governance failings in the sector will result in greater governance scrutiny/reporting arrangements for the college sector.

The Board of Management at Glasgow Kelvin College remains committed to maintaining high standards of corporate governance as evidenced in the recent Externally Facilitated Effectiveness Review report.

15. Risk Management Committee

At a recent Risk Management Committee meeting, due cognisance was taken of key risk reports/publications/newsletters; links provided below:

HEFESTIS Newsletters 5 November 2021 - 14 January 2022

The approved minute of the Risk Management Committee held on 2 November 2021 is provided for interest and perusal.

Risk Management Minute 02 November 2021

16. Resource Implications

There are some additional resource implications in relation to items referred to in this report i.e.:

- SFC Credit Funding clawback for 2021/22;
- negative implications of indicative SFC budget for 2022/23;
- overtime/cover costs arising as a consequence of staffing shortages due to the Covid19 pandemic and related implications;
- inspection of cladding at Springburn Campus;
- cost of additional security at our East End Community Garden;
- extremely high energy costs looming on the horizon;
- inflation/cost of living and food prices; and
- National Insurance increases (April 2022).

17. Risk & Assurance

The rising costs of energy, National Insurance contributions and food will have a severely detrimental impact on the poorest people in the societies we serve. There are real risks that people, already badly affected by the effects of the pandemic, will be placed under even more pressure by the rising costs of living. We can expect to see declining mental health, wellbeing, cold, illness and, sadly, hunger in the communities we serve. The College must strive to be a place of welcome relief and hope during these difficult times.

The introduction of new air-handling units will provide enhanced air quality throughout the Springburn Campus; this is particularly important in relation to Covid-19 and issues pertaining to ventilation improvement.

18. Equality

As aforementioned, the most deprived members of the communities we serve will be the most badly affected by the events we face nationally. People, already on the poverty line will feel the demands placed on already meagre resources. Demands on mental health services and food banks are at an all-time high. The College will strive to provide as many services to students as possible in an effort to make the campus buildings as welcome and pleasant as we can.

19. Data Protection

There are no issues arising from this report in relation to data protection. The College has put in place all Data Share Agreements and signage as per requirements.

20. Recommendations

Members of the Audit and Risk Committee are recommended to note the contents of this report, links and appendices provided for members information.

21. Further Information

Members can obtain further information on the contents of this report from Jeanette Evans, Vice Principal Operations at jevans@glasgowkelvin.ac.uk or Lisa Clark, Director of Corporate Services at lisaclark@glasgowkelvin.ac.uk

JE/LC
Glasgow Kelvin College - February 2022

GLASGOW KELVIN COLLEGE - Strategic Risk Register

Appendix 1

Board / Committee	
Prepared by: Jeanette Evans	
Contact Name and Tel. No.:	

						INHERENT ASSESSMENT					RESIDUAL ASSESSMENT										
Risk Ref No	**Date Identified**	**Risk Title**	Risk Description	**Risk Owner**	**Responsible Person**	**IL**	**II**	**IR**	**IR**	**Controls and Mitigating Actions**	**RL**	**RI**	**RR**	**RR**	**Risk Appetite Category**	**Risk Appetite**	**Risk Treatment Approach**	**Date Reviewed**	**Movement in Period**	**Early Warning Mechanisms, Planned Next Steps & Future Action Required**	**Date of Next Review**
1	04/11/2021	SFC Review	**RISK:** Being forced into position that is against our vision & mission, or reduces community engagement, e.g. A single governing body for Glasgow **CAUSE:** Failure to project a clear GKC identity or vision; failure to proactively engage in review; other voices are louder / stronger; or poor operating performance. **EFFECT:** Lose local autonomy; unable to meet local community needs; GKC identity is lost; loss of social footprint; loss of staff.	Principal & CEO / Chair	Vice Principal - Curriculum	4	5	20	**Very High**	1. Engagement with GCRB, SFC, Scot Gov, & UK Gov 2. Political engagement with local & national politicians 3. Engagement about possible models with other colleges 4. Board understanding & support 5. Identified forums where we can share our vision 6. Direct community engagement 7. Improved operating position & management of performance 8. Identifed awards & other opportunities to raise profile 9. Interaction with Scot Gov officials 10. Operational collaboration projects with other colleges	3	4	12	**High**	1. Policy	Cautious	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Outcome of consultants options appraisal 2. Ministerial responses / statements from Scot Gov 3. Performance Monitoring 4. GCRB Comms **Actions Planned** '1. Develop a college strategy for stakeholder consultation 2. Improving recruitment & student outcome performance 3. Continuing to influence GCRB decision making 4. Identify opportunities to collaborate	22.02.22
2	04/11/2021	GKC Identity	**RISK:** Lack of understanding or awareness of the critical part GKC plays in communities; don't communicate USP **CAUSE:** Do not proactively promote identity, successes & uniqueness of GKC; ineffective comms on identity & successes; failure to illustrate impact we have; underinvestment in marketing / messaging. **EFFECT:** Weak employer engagement; students choose another college; affects risk no. 1	Vice Principal - Operations		4	4	16	**Very High**	1. Tendering for new website 2. Developing new internal & external comms & marketing framework (in train) 3. Actively seeking to promote successes 4. Faculties using own social media 5. Investment in marketing resource 6. Employer engagement activity 7. Awards - putting forward GKC 8. Community Engagement, e.g. Hub 9. Digital strategy / My Kelvin	3	3	9	**High**	2. Reputation	Minimalist	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Negative publicity 2. Poor recruitment figures **Actions Planned** '1. Review of Comms & Marketing resource 2. Strategic Priority to raise profile 3. Campus Project 4. New website 5. Comms & Marketing Framework	22.02.22
3	04/11/2021	People	RISK: Not having agile, motivated, well-informed, or appropriately skilled workforce CAUSE: Demographics of workforce; national bargaining; NJNC notification of dispute; employment relations; lack of / insufficient CPD; failure to attract talented individuals; failure to retain talented individuals; unable to predict needs of the future; affordability of job evaluation. EFFECT: Unable to compete with industry; staff ability to be innovative is restricted; unable to deliver curriculum in areas of student demand; morale; financial stability.	Dir. Human Resources		5	4	20	**Very High**	1. People Strategy 2. Representation in employers association 3. NJNC negotiator 4. OD framework 5. TU engagement 6. RPA 7. TRCC 8. Recruitment & Retention Policies & Procedures 9. Culture of empowerment 10. 3 Year Rolling Budgets	2	2	4	**Medium**	5. Workforce	Cautious	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Staff turnover 2. Absences 3. HR Heatmap **Actions Planned** '1. Workforce Planning 2. Continuous improvement programme	22.02.22
4	04/11/2021	Litigation / Compliance	**RISK:** Non-compliance with key legislative or regulatory requirements **CAUSE:** Lack of awareness, understanding or training & development; poor compliance with established processes; not keeping up to date with changes in case law. **EFFECT:** Possible fines & litigation; reputational damage; implications for board accountability.	Dir of Corporate Services / & Dir Human Resources		4	4	16	**Very High**	1. Policies & procedures 2. Members of national groups to keep aware of developments & upcoming changes 3. Horizon scanning for changes to legislation or regulations 4. Legal advice 5. CPD programme 6. Staff training 7. Internal & external audit programme provides assurance 8. External DPO	1	3	3	**Medium**	7. Legal & Compliance (including Health & Safety risks)	Averse	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Horizon scanning 2. HR Heatmap 3. Compliance metrics **Actions Planned** '1. None Planned	22.02.22
5	04/11/2021	Curriculum Relevance	RISK: Curriculum doesn't meet current or future needs of students, employers, or community partners, or the economy CAUSE: Ageing workforce; lack of curriculum innovation; staff knowledge & expertise; People risk (Risk No. 3); employer engagement; outdated or lack of resources; unreliable information / data; growth of digital teaching / you tube. EFFECT: Diminishing recruitment; reputation; student achievement; reputation.	Vice Principal - Curriculum		4	4	16	**Very High**	1. Curriculum reviews 2. Staff training / CPD 3. Emp engagement 4. Schools engagement 5. Partners - HE 6. Labour market intelligence 7. Staff structures / PDR 8. Industry bodies 9. Student feedback 10. Collaboration with partners & colleges 11. Digital transformation	3	3	9	**High**	6. Student Experience	Open	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Recruitment & retention of students 2. Emp & student feedback 3. Success rates **Actions Planned** '1. Strengthen CPD for staff 2. Strengthen Curriculum review 3. Digital / blended development 4. Targeted emp engagement 5. Creation of Centres of Excellence 6. Green Kelvin	22.02.22
6	04/11/2021	Sustainable Funding	RISK: Inability to secure appropriate levels of funding to deliver objectives. CAUSE: constraints of current funding structures & levels; budget cuts; Scot Gov / SFC funding models; constraints in public finances; non-compliance; Foundation Apprenticeship arrangements changing, re-distribution of credit activity for 2021-22; NI costs rising, inflation high, energy prices soaring. EFFECT: loss of income; inability to deliver financially sustainable budgets; med-long term sustainability at risk; impact on curriculum delivery; job losses	Vice Principal - Operations		4	4	16	**Very High**	1. 3 year budgets 2. Management accounting & budgetary control 3. Quarterly budgets & forecasting 4. TRCC 5. Compliance framework - review, monitor & control of funding obligations 6. Annual internal audit programme 7. Funding officer in Business Development team 8. Underlying cash position to agreed levels. 9. ~~Building up cash position~~ 10. ~~Building~~	4	3	12	**High**	3. Financial	Cautious	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Negative variances 2. quarterly reviews 3. Budget reviews 4. Nov SFC Nov cut-off **Actions Planned** '1. Enhancing business intelligence on funding streams 2. Building ALF 3. Curriculum planning 4. Identify alternative funding streams / Business Development Ambitions	22.02.22
7	04/11/2021	Student Experience	**RISK:** Poor student experience **CAUSE:** Poor physical environment; quality of teaching; lack of teaching skills or resources; lack of support services **EFFECT:** Impact on retention of students; reputational damage among possible future students; financial instability; performance outcomes affected; relationship with employers; failure to deliver Government ambitions	Vice Principal - Curriculum		4	4	16	**Very High**	1. Curriculum quality assurance 2. Quality framework 3. Curriculum Planning 4. Student feedback 5. Engagement with Student association 6. Learning & support services 7. CPD for staff 8. Investment in estate 9. Planned & routine maintenance 10. Operational planning process has Student Engagement at heart 11. GTCS Strategy	3	3	9	**High**	6. Student Experience	Open	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Student numbers metrics 2. Student destination **Actions Planned** '1. Campus Project 2. Retention improvement plan 3. Quality system review & development 4. Business Intelligence reporting & monitoring 5. Learner engagement 6. GTCS Strategy	22.02.22
8	04/11/2021	Environment	**RISK:** College fails to meet targets in relation to sustainability, e.g. Net Zero **CAUSE**: Lack of resources to implement; lack of skills to implement; sustainability is not embedded within curriculum; cannot access funding; limited by pace of industry **EFFECT**: Do not meet targets; impact on future generations; reputation with students, future students, community & government affected	Vice Principal - Operations / Director of Corporate Services		4	4	16	**Very High**	1. Public Sector Climate Change Report completed annually. 2. Funding to recruit Environmental Manager secured from the SCIO for 2 years. 3. Individual appointed and start date awaited. 4. Environmental Manager will raise environmental awareness & access funding streams. 5. Green Kelvin initative is a key strategic priority. 6. Awareness raising activity paramount.	3	3	9	**High**	8. Environmental Sustainability	Minimalist	Treat	04/11/2021	New	**Early Warning Mechanism** 1. PSCC metrics **Actions Planned** '1. Recruitment of Environmental Manager 2. Implementation of Green Kelvin action plan 3. CPD 4. Curriculum changes	22.02.22
9	04/11/2021	Digital Transformation	**RISK:** Inability to deliver Digital Transformation Strategy & Programme **CAUSE:** Lack of resources to implement; lack of skills to implement; user skills insufficient; poor change or project management **EFFECT:** Reputation with students & staff affected; operational effectiveness reduced; student experience deteriorates	Vice Principal - Curriculum		4	4	16	**Very High**	1. Strategy & Programme 2. Staffing structure to support delivery 3. Increased resources to implement 4. Staff training & awareness 5. New software 6. Website tendering 7. Increased devices available to staff & students 8. Programme management / governance	2	3	6	**Medium**	4. Digital	Cautious	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Missed deadlines / milestones **Actions Planned** '1. Implementation of programme: further development of business intelligence for learning & teaching development 2. Continuation of staff training	22.02.22
10	04/11/2021	Student Recruitment & Retention	**RISK:** Fail to Recruit or Retain Sufficient students or learners **CAUSE:** Effectiveness of admissions process; monitoring of information; lack of identity; ineffective marketing; curriculum offer does not meet student needs **EFFECT:** Students do not get access to quality learning & teaching; class sizes are not sustainable; reduced funding; additional expenditure; COVID-19 mental health challenges.	Vice Principal - Curriculum		5	4	20	**Very High**	1. Admissions process 2. Marketing 3. Monitoring attendance & performance 4. Wellbeing Lead appointed to engage with student body.	3	4	12	**High**	6. Student Experience	Cautious	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Student recruitment metrics 2. Drop out metrics **Actions Planned** '1. 2. 3.	22.02.22
11	04/11/2021	Cyber Risk	**RISK:** A widespread cyber-attack breaches college defence **CAUSE:** A malicious breach of college systems possibly caused by: user error / lack of training or education; lack of patch management; failure of perimeter security; poor development practices; lack of investment in protection **EFFECT:** Loss of business critical systems; college reputation damaged / loss of credibility; impact on individual people (data subjects); possible fines or litigation; cost to repair or restore; impact on students / student experience	Vice Principal - Curriculum		5	5	25	**Very High**	1. Automated patch management 2. Mandatory training for all college employees 3. Firewall & DNS protection 4. MFA (multi-factor authentication) controls 5. Safelinks 6. Information security policy 7. Anti-virus & malware scans 8. Development frameworks 9. Knowledge sharing with peers 10. Cyber security insurance 11. Disaster Recovery / Business Continuity Plan in place - including backups	3	4	12	**High**	2. Reputation	Minimalist	Treat	04/11/2021	New	**Early Warning Mechanism** 1. Monitoring of key systems performance & availability 2. Log management / monitoring 3. Monitoring of open source cyber intelligence, websites etc. **Actions Planned** '1. Review need for zero-trust architecture 2. Review how embedded mandatory training is for all staff	22.02.22
12	13/12/2022	COVID-19 - Ongoing Implications	**RISK:** Ongoing negative impact of COVID-19 on all aspects of College operations. **CAUSE:** New virus strains causing higher/ongoing levels of staffing absence due to illness/self-isolation. Staff members at work feeling under increased pressure. Individuals living in a constant state of fear for circa 2 years has resulted in mental health deterioration/issues related to anxiety/lack of confidence. Return to study/work/hybrid model causing feelings of unease. **EFFECT:** Loss of business, reduced student learning experience, higher than normal drop out rates/absence; high costs for staff cover, college reputation damaged/loss of credibility; very negative impact on different groups of people.	Principal & CEO / Chair		5	5	25	**Very High**	1. Discussions taking place about a hybrid model of working to enable people to start to think about this. 2. Enhanced cleaning regime remains in place throughout the campus buildings. 3. Social distancing in place. 4. Rooms ventilated if at all possible; upgrade to ventilation system at Springburn Campus. 5. Low numbers of people in campus buildings/hybrid working will ensure this is still low. 6. Signage in place. 7. Anti-virus hand sanitiser and wipes available across the entire campus. 8. Masks available. 9. External signage. 10. LFD tests available. 11. Wellbeing high on the agenda for the College student and staff population.	3	4	12	**High**	1. Policy	Cautious	Treat	13/12/2022	New	Early Warning Mechanism 1. Monitoring of Scottish Government messages. 2. Management/monitoring of staffing situations. 3. Monitoring of positive test cases/health issues. Actions Planned 1. Keeping abreast of Scottish Government's guidance. 2. Keep a close watch on staffing levels and cover required.	25/01/2022

Likelihood

TITLE	DESCRIPTION	SCALE
Almost Certain	Very high chance, or even certainty, that this will happen	5
Likely	Likely to happen	4
Possible	Possible chance of happening	3
Unlikely	Small chance of happening	2
Rare	Very unlikely. Assumption is that it will never occur	1

Consequence

TITLE	DESCRIPTION	SCALE
Catastrophic	Death, total systems loss, unacceptable outcome	5
Major	"Major" injury/illness, major damage or impact	4
Moderate	Loss time injury/illness, serious damage or impact	3
Minor	Minor impact or outcome	2
Insignificant	Very minor. Little consequence	1

Likelihood x Consequence

13 - 25	Critical risk – should be eliminated or moved to a lower level
8 - 12	Undesirable – must be avoided if reasonably practicable
3 - 7	Acceptable – can be accepted provided risk is managed
1 - 2	Low -no further consideration required

	Risk remains above acceptable level
	Risk remains undesirable
	Risk is acceptable or can be managed

↑	Increasing Trend
↓	Decreasing Trend
↔	Constant Trend

Risk Appetite Statement

This statement specifies the Risk Appetite or willingness of the Board of Management to accept or tolerate different types of risk. The Board is responsible for the overall management of risk and opportunity. It sets the risk appetite and ensures there is an appropriate balance between risk and opportunity and that this is communicated to the management team.

The Board of Management are Risk Minimalist in respect of all matters which involve the stewardship of College funds and our reputation. It is risk averse in compliance with legislation. This includes compliance with high standards of health & safety management. The College is a dynamic and innovative educational institution which is willing to accept a level of risk as it seeks to identify new ways of working which will improve the quality and range of services it offers to the communities which it serves.

The Risk Appetite Statement is integrated with the Risk Register and will be taken account of on all occasions the Risk Register is considered by the Board of Management, its Audit and Risk Committee and its other Standing Committees. At each review of the Risk Register the level of mitigation must be considered against the assessed level of Risk attached to any item on the Risk Register and the Risk Appetite applicable to it.

	Risk Appetite				
Risk Category	**Averse**	**Minimalist**	**Cautious**	**Open**	**Hungry**
1. Policy					
2. Reputation					
3. Financial					
4. Digital					
5. Workforce					
6. Student Experience					
7. Legal & Compliance (including Health & Safety risks)					
8. Environmental Sustainability					

Appendix 2 – Air Handling Unit Installation at Springburn Campus

Crane arrival and set up

Loading and positioning of air handling unit

Appendix 3 – East End Community Garden – Vandalism/CCTV Tower

Recycling Bins prior to vandalism

Damage caused to Bins

Example of CCTV Tower

Area of camera coverage

CCTV Signage

CCTV Signage in place

Scottish colleges: 'Governance questions still to be answered'

COMMENT

There is growing concern over governance arrangements for Scotland's colleges.

0 comment

ADVERTISEMENT

In 2015, the board of management of Glasgow Clyde College was removed by the Scottish Government following "repeated incidences of failure relating to governance".

Scottish ministers at that time assured us that important lessons had been learned. Angela Constance, then Cabinet Secretary for **Education**, commissioned a report that made recommendations to improve governance across the sector.

These recommendations, we were told, would be adopted by the Scottish Government and the Scottish Funding Council to ensure early intervention if required, and ongoing good governance in Scotland's colleges. It remains unclear which, if any, of these recommendations, have been implemented.

Compare that commitment from our recent past with the unfolding situation at South Lanarkshire College (SLC), where staff at the college have raised concerns regarding allegations of misconduct involving some of the previous management team. These staff concerns, in turn, led to a thorough and forensic investigation being commissioned by the recently-appointed college principal in 2020.

READ MORE: MSPs urged to intervene over college 'misconduct' report

While this investigation was in the process of being undertaken, two senior managers involved in overseeing that investigation were suspended by the college board of management. The findings of the investigation mentioned have not been made public and staff are deeply concerned by the actions of this college board.

The role of the Scottish Funding Council in this matter remains unclear. Despite having conducted "a governance review" at the college in the summer of 2021 at the instigation of the principal, the report has never been made public. The report also appears not yet to have been progressed by the board.

According to its most recent statement, the Scottish Funding Council appears reluctant to become involved in this crisis, and has chosen to defer responsibility to the SLC and Lanarkshire regional boards.

Angela Constance is a former Scottish education secretary.

Staff at SLC have also reacted strongly to the current situation within the college, whereby two senior staff – the clerk to the board, and the principal – have been suspended.

In November, the staff passed a unanimous vote of "no confidence" in the college chair, and more recently – following the board's decision to suspend the two staff members – voted similarly regarding the entire SLC board.

College staff have also demanded an end to the suspension of the clerk to the board, and the college principal. It is understood that a number of staff complaints against board members, and also regarding college governance, have not been actioned, despite being formally submitted in accordance with college procedures some months ago.

READ MORE: Funding council under pressure as crisis deepens at college in 'misconduct' storm

The situation at SLC raises several questions for the Scottish Government:

- What has been learned from previous instances of poor governance in the further education (FE) sector?

- Where was the early intervention from the Scottish Funding Council to ensure effective governance and transparency at SLC?
- What will be the cost to the public purse of the SLC board's actions?
- How many **law** firms are now engaged by the FE sector in the Lanarkshire region, and at what cost?

All of the above are important questions for the system that purports to oversee and ensure that good governance prevails within public bodies in **Scotland**.

So far, staff at SLC, and no doubt throughout the FE sector, are certain that this system has failed to provide adequate answers.

The author is a Scottish FE lecturer who asked not to be named.

Scotland 'racing headlong into a teen gang crisis' with kids 'as young as 11 tooling up with knives'

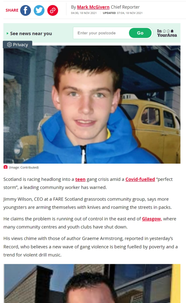
Closure of youth clubs is pushing more youngsters into the streets, claims a leading community worker.

SHARE

By Mark McGovern Chief Reporter
Email: 5 mins ago | Updated: 1 hour ago

NEWS

+ See news near you
Enter your postcode Go
Sponsored by Yourlens

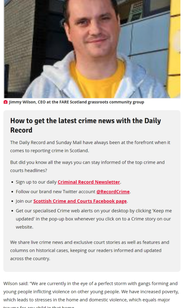


Scotland is racing headlong into a teen gang crisis amid a Covid-fuelled "perfect storm", a leading community worker has warned.

Jimmy Wilson, CEO at FAME Scotland grassroots community group, says more youngsters are arming themselves with knives and roaming the streets in packs.

He claims the problem is running out of control in the east end of Glasgow, where many community centres and youth clubs have shut down.

His views chime with those of author Graeme Armstrong, reported in yesterday's Record, who believes a new wave of gang violence is being fuelled by poverty and a trend for violent drill music.


Jimmy Wilson, CEO at the FAME Scotland grassroots community group

How to get the latest crime news with the Daily Record

The Daily Record and Sunday Mail have always been at the forefront when it comes to reporting crime in Scotland.

But did you know all the ways you can stay informed of the top crime and courts headlines?

- Sign up to our daily Criminal Record Newsletter.
- Follow our brand new Twitter account @RecordCrime.
- Join our Scottish Crime and Courts Facebook page.
- Get our specialised Crime web alerts on your desktop by clicking 'Keep me updated' in the pop-up box whenever you click on to a Crime story on our website.

We share live crime news and exclusive court stories as well as features and columns on historical cases, keeping our readers informed and updated across the country.

Wilson said: "We are currently in the eye of a perfect storm with gangs forming and young people inflicting violence on other young people. We have increased poverty, which leads to stresses in the home and domestic violence, which equals major trauma for any child in that home.

"We are seeing the mass closures of community centres, meaning what youth clubs there were in deprived areas are shutting down.

Gang pictures posted on social media

"It sounds like a cliche but there's never been a time in recent memory like this, when you could say that young people have got nothing to do.

"Kids as young as 11 are getting tooled up with knives and it's made worse by the internet, where all that stuff gets glorified. They are reviving the names of the old gangs you've barely heard of in years – and that's something we have to dread."

Get local news and info
Enter your postcode to see news and information near you
Enter your full postcode Go
Sponsored by Yourlens | Privacy Policy
Get it on Google Play | Download on the App Store

A picture sent to the family of murdered Jonathan McLaughlin by rival gang thugs posing beside the tributes left at the scene of his death.

"There have been some well publicised incidents and there was a boy left in a coma in hospital the day before Justin McLaughlin's death."

Wilson said Glasgow City Council's list of community centres that have shut down is hard to believe.

READ MORE
Gold fitting gang of yobs stealing e-bikes worth £8K from garden in broad daylight

TOP NEWS STORIES TODAY
Brave Scots mum abused by cop boyfriend
Billie John photos could lead to killer
Scots school racked by new abuse claims
Cops tape off part of Hamilton

He is seeking funding for initiatives that will operate within schools in tough communities and run for three to five years.

A spokesperson for Glasgow Life acknowledged the huge scale of closures.

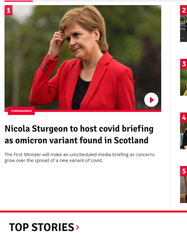
He said: "The £100million funding guarantee we received from Glasgow City Council in March 2021 allowed us to give reopening dates for more than 90 venues but we can't open more without more funding."

Follow Daily Record

Facebook Twitter

MORE ON
Coronavirus Glasgow Teenagers Organised Crime

NEWS ALL
Most Read Most Recent

1

CORONAVIRUS
Nicola Sturgeon to host covid briefing as omicron variant found in Scotland
The First Minister will make an unscheduled media briefing as concerns grow over the spread of a new variant of covid.

2

HAMILTON
Young woman's body found in Hamilton woods as police probe death

3

CORONAVIRUS
Covid in Scotland LIVE as Nicola Sturgeon calls for tougher travel restrictions

4

CORONAVIRUS
NHS nurse who branded covid 'scamdemic' sacked for posting conspiracy theories

5

CORONAVIRUS
Nicola Sturgeon calls for tougher travel restrictions as concerns grow over omicron covid variant

CUDONI
BLACK FRIDAY WEEKEND
25% OFF GUCCI
LOUIS VUITTON
PRADA & MORE

RECOMMENDED
Nicola Sturgeon to host covid briefing as omicron variant found in Scotland
Young woman's body found in Hamilton woods as police probe death
Covid in Scotland LIVE as Nicola Sturgeon calls for tougher travel restrictions
NHS nurse who branded covid 'scamdemic' sacked for posting conspiracy theories
Nicola Sturgeon backs tougher travel restrictions as new omicron covid variant

e-on
We're saving 99 million tonnes of CO2 a year. Together we can save more.
LEARN MORE

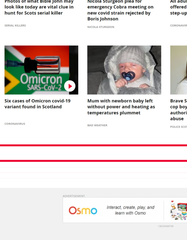
RECOMMENDED
Doctor who raised concern over Omicron variant says symptoms are 'unusual'
Teenager charged with murdering schoolgirl Ava White
Cops cordon off secluded area near Hamilton town centre as officers hit on phones
Photos of what Billie John may look like today after manhunt for serial killer

e-on
We're saving 99 million tonnes of CO2 a year. Together we can save more.
LEARN MORE

RECOMMENDED
Six cases of Omicron could 19 variant found in Scotland
Brave Scots mum terrorised by cop boyfriend calls on authorities to tackle domestic abuse
First pic of Scots mum found dead at home as police ex-cop man
What did Nicola Sturgeon say on today's Covid briefing - seven important updates

Shark
BLACK FRIDAY EVENT
SAVE UP TO £250
EXCLUSIVE BUNDLE
Shop Now
DETOMASO
LIMITED EDITION
SHOP NOW

TOP STORIES


Man charged in connection with death of young Scots mum found in Stirling home
STIRLING

Campaign for Scottish independence to resume 'in earnest' next year, says Nicola Sturgeon
INDEPENDENCE REFERENDUM

Scot with schizophrenia challenged over whether he was 'safe' around kids
EAST KILBRIDE

Nicola Sturgeon calls for tougher travel restrictions as concerns grow over omicron covid variant
CORONAVIRUS

Photos of what Billie John may look like today are vital clue in hunt for Scots serial killer
SERIAL KILLERS

Nicola Sturgeon plea for emergency Cobra meeting on new covid strain rejected by Boris Johnson
NICOLA STURGEON

All adults in Scotland to be offered covid booster in huge step-up of vaccination campaign
CORONAVIRUS

Man charged after alleged murder BoF at East Kilbride shopping centre
POLICE SCOTLAND

Six cases of Omicron covid-19 variant found in Scotland
CORONAVIRUS

Mum with newborn baby left without power and heating as temperatures plummet
BAY HEATER

Brave Scots mum terrorised by cop boyfriend calls on authorities to tackle domestic abuse
POLICE SCOTLAND

Nicola Sturgeon announces £20 a week anti-poverty payment for low income families
POVERTY

ADVERTISEMENT
Osmo
Interact, create, play and learn with Osmo
15% off voucher
Osmo - Little Genius Starter Kit for Fire Tablet + 3 Educational Learning Games - Preschool ...
Powered by Amazon

HEFESTIS Weekly Newsletter

In this week's threatscape we highlight an increase in phishing campaigns targeting the HE/FE sector, a brute force attack against one of our members, a ransomware update, recent vulnerabilities and common insider threats.

Here are some of the week's Cyber Security articles which caught the attention of CISO-Share.

Increase in Phishing campaigns targeting HE/FE

A number of HEFESTIS members have experienced phishing campaigns that follow a similar pattern. The attacker uses compromised user credentials to log into Microsoft 365 email. They then use this access to send bulk phishing emails to internal and external contacts.

The bulk emails contain a link to a credential harvesting website designed to trick users into entering their login details. So far COVID and research related themes are prevalent within the phishing scripts. There has also been reported a co-ordinated brute force attack synchronised with elevated phishing activity.

If you are a member and experience a similar attack, then reference the following playbooks.

Phishing Playbook

Account Compromise

Report any Phishing URLs for takedown at:
https://www.ncsc.gov.uk/section/about-this-website/report-scam-website.

Reset affected passwords and check logs for remote access and malicious activity from all compromised accounts within the timeline of the attack.

Fortunately, standard countermeasures and protections as recommended by HEFESTIS CISO-Share are proving effective in mitigating this current activity.

Protections against these types of attack include MFA, good password management and user awareness. O365 security tools can detect and help eradicate the reported incidents, which all appear to have been contained at this time.

Action Point:

If there is anyone, member, or non-member, who is struggling with how to respond to a cyber incident or needs help, guidance, advice, or even good old-fashioned support, then PLEASE reach out to us.

We exist to serve the HE/FE community, members or not, especially at a time when our sector is under increased attack.

Please do not wait until an incident occurs, if you are unsure, then please make contact.

Our contact details are as follows.

Steve McIntosh	David Robertson	Darren Clement
M: 07904 908945	M: 07852 330122	M: 07442 859979
E: smcintosh@hefestis.ac.uk	E: drobertson@hefestis.ac.uk	E: dclement@hefestis.ac.uk

---

Common Types of Insider Threats

https://www.securelink.com/blog/common-types-of-insider-threats-that-can-cause-breaches/

The Verizon 2020 Data Breach reports that insiders account for 22% of all security incidents. A survey by the Ponemon Institute found that the overall cost of insider threats rose from $8.76 million in 2018 to $11.45 million in 2020, representing a 47% increase in two years.

The main goals or categories of insider threats:

- **Fraud** – an insider will steal, modify or destroy data for the purpose of deception.
- **Sabotage** – an insider will use their legitimate access to the network to destroy or damage the company systems or data.
- **Espionage/spying** – an insider steals company data or information for another organization such as a government entity or competitor.
- **IP Theft** – an insider steals a brand or company's patents, designs, inventions, etc., often taking them to a new company or for resale.

There are many types of insider threat actors. Such as:

Malicious Insiders often have an unsolved grievance against the company they work for and they choose to take things into their own hands. Malicious insiders can work solo or in organised groups.

Careless Employees are not aware of the many security implications that their behaviours have in reducing the security of their organisations.

Third-Party Partners sometimes do not have sophisticated security protocols and are easy targets for cyber attackers.

Ex-Employees may be leaving the company involuntarily and decide to steal valuable data.

Policy Evaders who like to take shortcuts when it comes to following security policies and protocols.

Action Points:

- Educate your users and business partners on cybersecurity.

- Thoroughly vet who you are going to partner with based on the maturity of their cybersecurity model.
- Invest in the right cybersecurity tools and technologies as countermeasures against internal data breaches.

New 'Shrootless' vulnerability on macOS Systems

https://thehackernews.com/2021/10/new-shrootless-bug-could-let-attackers.html/

The vulnerability is called "Shrootless" and tracked as CVE-2021-30892, the vulnerability lies in how Apple-signed packages with post-install scripts are installed.

Successful exploitation of CVE-2021-30892 could enable a malicious application to modify protected parts of the file system, including the capability to install malicious kernel drivers (aka rootkits), overwrite system files, or install persistent, undetectable malware.

Action Point:

- Apple said it remediated the problem with additional restrictions as part of security updates pushed on October 26, 2021. So ensure that this update is installed.

40% of organizations have suffered a cloud-based data breach

https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-data-breach

The 2021 Thales Global Cloud Security Study reports that one-fifth (21%) of businesses host most of their sensitive data in the cloud, and 40% of organizations have experienced a cloud-based data breach in the past 12 months. 33% report multi-factor authentication (MFA) as a central part of their cybersecurity strategy. However, only 17% of those surveyed have encrypted more than half of the data they store in the cloud.

Half (46%) of global respondents claim managing privacy and data protection in the cloud is more complex than on-premises solutions.

Cybercriminals and nation-state attackers are targeting cloud services more than ever before, and consequently, organizations must prioritize cloud security to make it difficult for attackers to be successful.

Action Point:

- Organisations must adopt a cloud security strategy designed to reduce the risks of cloud assets, such as data encryption, multi-factor authentication (MFA) and privileged access security.

- Organisations must evaluate what security is available and ensure they move to security by default.

Cybercrime: Europol arrests 12 people for ransomware activities

https://www.techrepublic.com/article/cybercrime-europol-arrests-12-people-for-ransomware-activities-possibly-affecting-1800-victims-in-71-countries/

Europol, the European police agency, announced today the arrests of 12 people involved in ransomware activities across the world. The alleged cybercriminals are believed to have affected over 1,800 victims in 71 countries according to Europol's press release; those victims are mostly large corporations and critical infrastructures. Norwegian National Criminal Investigation Service, commonly known as Kripos, communicated and reported that one of the victims was Hydro, back in March 2019.

The operation took place on Oct. 26 in Ukraine and Switzerland. In addition to the arrests, law enforcement seized five luxury vehicles, over $52,000 and electronic devices that will be analysed forensically to add to the investigation and possibly bring new investigations.

Action Points:
Recommendations for how to detect and prevent ransomware

- Use multi-factor authentication whenever possible. As cybercriminals often gain access to a system by gaining legitimate user credentials, MFA can help protect the system by forbidding the criminals to log in using a legitimate user account.
- Don't let sensitive data be accessible via the internet. Data isolation is important and needs to be done continuously.
- Have a safe backup system for all important data. Also remember that attackers often deactivate backup systems before attacking, so any change to the backup politics need to raise alerts to the security staff.
- Make sure all your applications and assets are up to date, and apply patches as fast as possible to avoid being victimized via a software vulnerability.
- Work with a zero-trust strategy. Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. It helps to enforce least privilege access across all applications, cloud platforms, systems and databases.
- Audit your system for vulnerabilities to help ensure that cybercriminals will not use any easy software or misconfiguration to penetrate the corporation.
- Raise employees' awareness by running security campaigns to educate them, and focus on phishing emails, since it is one of the most common way to initially compromise a system.

---

10 ways ransomware attackers pressure you to pay the ransom

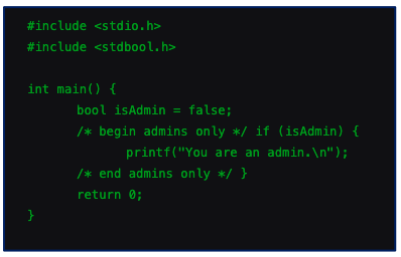
https://www.techrepublic.com/article/10-ways-ransomware-attackers-pressure-you-to-pay-the-ransom/

The Main article lists all 10 additional exploitation tactics.

Cybercriminals who employ ransomware have gotten much bolder in recent years. Beyond stealing sensitive data, such criminals will turn to a variety of tactics to further persuade the victim to pay the ransom. A new report from security firm Sophos look at 10 ways attackers pressure organizations to pay the demanded ransom. The report also includes recommendations on how to defend yourself against these types of attacks.

Action Point:

In the past, ransomware was a relatively straightforward matter. An attacker would breach an organization and encrypt critical data. Without a reliable or recent backup, that organization would have few options other than to pay the ransom in the hopes that the data would be decrypted. Now, however, organizations have gotten more diligent about backing up important data, which means they may be less likely to pay the ransom. As a result, cybercriminals have turned to more aggressive and forceful tricks to demand that the ransom be paid.



```
#include <stdio.h>
#include <stdbool.h>

int main() {
	bool isAdmin = false;
	/* begin admins only */ if (isAdmin) {
		printf("You are an admin.\n");
	/* end admins only */ }
	return 0;
}
```

'Trojan Source' Attack Abuses Unicode to Inject Vulnerabilities Into Code

https://www.securityweek.com/trojan-source-attack-abuses-unicode-inject-vulnerabilities-code

Researchers from the University of Cambridge have identified a new attack method that abuses Unicode to stealthily inject vulnerabilities into code.

Dubbed Trojan Source, the attack impacts many of the compilers, interpreters, code editors, and code repository frontend services used by software developers.

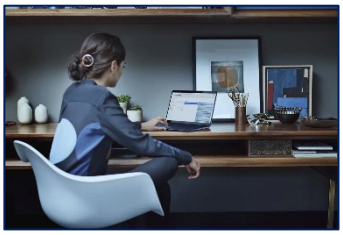
Unicode is the standard for the consistent encoding, representation, and handling of text in most of the world's writing systems. Some languages are written left-to-right (e.g. English) and others right-to-left (e.g. Hebrew and Arabic). However, Unicode provides a feature — named the Bidirectional (Bidi) Algorithm — for when two types of writing need to be mixed. For example, writing a single word from a right-to-left language in a sentence written in a left-to-right language.

Action Point:

The Cambridge researchers have scanned publicly available source code in an effort to find signs that the Trojan Source attack has been exploited for malicious purposes. While there is no evidence of Trojan Source attacks in the wild, they did see similar techniques being exploited, although many were not necessarily malicious.

The researchers have provided recommendations for preventing abuse and said half of the compiler maintainers they have contacted are either working on patches or have promised to do so.

Rust developers have already released an update that should prevent attacks, and they have published an advisory describing impact.



IT Teams Say Work from Home Is a 'Ticking Time Bomb'

https://www.csoonline.com/article/3639034/new-hp-wolf-security-report-83-of-it-teams-say-work-from-home-is-a-ticking-time-bomb.html

The latest HP Wolf Security study – *Rebellions & Rejections* highlights that if employees don't understand the goals and reasoning behind their organization's security policies – and if technical controls are too obtrusive – this can lead to apathy, resentment, and even circumvention.

Key Findings

- 76% of IT teams polled admit security took a back seat to business continuity during the pandemic, while 91% felt pressure to compromise security if it benefitted business continuity.
- Almost half (48%) of younger office workers (18-24 years old) surveyed viewed security tools as a hindrance, leading to nearly a third (31%) trying to bypass corporate security policies to get their work done.
- 48% of office workers surveyed agreed that seemingly essential security measures result in a lot of wasted time – rising to 64% among those ages 18-24.
- Over half (54%) of 18–24-year-olds were more worried about meeting deadlines than exposing their organization to a data breach; 39% were unsure what their security policies say, or are unaware if their company even has them – suggesting growing apathy or a lack of awareness among younger workers.
- As a result, 83% of IT teams surveyed believe the increase in home workers has created a "ticking time bomb" for a corporate network breach.

Action Points:

- Implement security controls with transparency, usability, and digital transformation in mind.
- Build a collaborative security culture. Effective security governance relies on users complying and engaging with security policies.

Digital natives more likely to fall for phishing attacks at work than their Gen X and Boomer colleagues

https://www.techrepublic.com/article/digital-natives-more-likely-to-fall-for-phishing-attacks-at-work-than-their-gen-x-and-boomer-colleagues/

SailPoint survey finds that younger workers also are more likely to use company email addresses for online shopping and subscriptions.

A new Trust Issues survey found that Gen Z and Millennials should follow the example set by their elders to develop better cyber hygiene habits at work. This SailPoint survey asked 500 U.S. workers about how they use email and deal with phishing attacks.
The survey asked how respondents reacted to a suspicious looking email with a link or an attachment. Forty-six percent of Gen Z respondents said they would open the link or attachment, compared to just 1% of Boomers, 4% of Gen X and 29% of Millennials who also would take the bait.

Sailpoint CISO Heather Gantt-Evans said digital native generations have a different comfort level with what they engage with and post online, compared to people who can remember the days of dial-up or even no internet access at all.

Action Point:

Gantt-Events recommends implementing the following tactics to mitigate the risk of phishing and other common attacks:

- Limit Remote Desktop Protocol use and ensure it is behind VPN with MFA
- Establish email hygiene, browser isolation and endpoint detection and response capabilities
- Conduct regular phishing awareness training with regular phishing tests
- Use "external" markers in the subject line for emails from outside the organization
- Add a phish report button to email clients
- Patch all software in a timely manner and ensure software centres and golden images have up-to-date versions

---

Brute force attack: A brief user story from one of our members

The information bellow is not public knowledge yet, however the authoring institution, who would prefer to stay anonymous for now, is keen to share the following information with the membership which may be of value to some or all of you.

Malicious activity - particularly a lot of brute-force attack on IMAP4 and SMTP has been experienced at this institution. All users have been informed.

The institution has the full MS Defender suite and reports dozens of accounts that were directly targeted via brute force attack *Microsoft Cloud App Security only reported 2.

The brute-force was ongoing for days with Microsoft recommending the enabling of MFA on all accounts only to have it pointed out that MFA does not work on legacy protocols.

More helpfully, on the Microsoft website the recommendation was of disabling legacy protocols with a Conditional Access policy as it is easy.

The only problem with this mitigation is that CA policies are only evaluated **after** a successful logon.

It was decided that the most effective means by which to protect the environment was to initiate the lockout policy, which would slow the malicious brute force activity down but would not stop it.

By the end of Monday 3 patterns were reported:

- Noisy IMAP4 with IPs from all over (mainly China, Russia, South America, Eastern Europe)
- Slow IMAP4 (approx. a logon at every 20 minutes, mainly from JP)
- Slow SMTP on some Marketing, etc shared accounts.

A good place to check for activities is "Usage & insights" in AAD and selecting "Office 365 Exchange Online".

The organisation were in the process of disabling legacy authentication using CA, so it was partially deployed. However, due to the fact that you need a successful logon for the CA to work, they moved into disabling Legacy Authentication at EOL level using policies. The advantage of this is that you also stop seeing the failed authentication logs (i.e. Azure AD logs don't get cluttered)

The disadvantage of disabling legacy authentication is that, in this instance, most iPhone users use Activesync and their email stopped working.
If this is an issue, the reporting organisation recommends installing Outlook as this will come handy when we move into DLP as policies can be applied and Outlook will respect them.

Action Point:

The disadvantage of disabling legacy authentication is that iPhone users using Activesync may experience their email stopping working.

If this is an issue, the reporting organisation recommends installing Outlook as this will not only resolve the issue for iPhone users but will come in handy for Data Loss Prevention activity as policies can be applied and Outlook will respect them.

Hardcoded SSH Key in Cisco Policy Suite Lets Remote Hackers Gain Root Access

https://thehackernews.com/2021/11/hardcoded-ssh-key-in-cisco-policy-suite.html

Tracked as CVE-2021-40119, the vulnerability has been rated 9.8 in severity out of a maximum of 10 on the CVSS scoring system and stems from a weakness in the SSH authentication mechanism of Cisco Policy Suite.

A successful exploit could allow the attacker to log in to an affected system as the root user.

Cisco Policy Suite Releases 21.2.0 and later will also automatically create new SSH keys during installation, while requiring a manual process to change the default SSH keys for devices being upgraded from 21.1.0.

Change the Default SSH Keys

To generate new SSH keys and propagate them to all the machines in the deployment, follow these steps:

Step 1

To generate new keys, execute the following command on installer VM (Cluster Manager):

```
/var/qps/install/current/scripts/bin/support/manage_sshkey.sh --create
```

Step 2

Update keys on CPS VMs and installer VM (Cluster Manager):

```
/var/qps/install/current/scripts/bin/support/manage_sshkey.sh --update
```

Action Point:

- Update and renew keys for any affected CISCO devices.
- Also released were multiple vulnerabilities affecting the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT). https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr

---

Recently released

	HEFESTIS Briefing Note – Credential stuffing prevention – CNIL enforcement
	Data Protection & Security 2021
	Cyber Attack Evolution 1
	Cyber Attack Evolution 2
	How to know you've been attacked

	How to respond to an attack
	Human Factor
	TTX Overview
	Ransomware Preparedness
	Supplier Security
	Breach Management Risks and Notification
	Data Protection by Design and Default
	Trusted Third Parties
	Data Breaches 1
	Data Breaches 2
	Ransomware preparedness checklist
	Acco unt Security Advisory
	Business Continuity Planning Webinar, presentation slides
	Business Continuity Planning Webinar, presentation recording
	Business Continuity Cheat Sheet
	BIA – HR System – Scotia University (template and example)
	Business Continuity Plan Template
	CRF 17. Business Continuity – HEFESTIS Breakdown

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Weekly Newsletter

In this week's threatscape we highlight endpoint security, the growing threat to Operational Technology, 2022 predictions from the RSA conference, increased DDoS activity and the latest vulnerabilities of concern.

Here are some of the week's Cyber Security articles which caught the attention of CISO-Share.

Palo Alto Networks patches 9.8 severity CVE in popular GlobalProtect product

https://www.theregister.com/2021/11/11/palo_alto_networks_critical_cve_globalprotect/

Palo Alto Networks (PAN) has issued a patch for a CVSS 9.8-rated buffer overflow affecting a VPN component of its widely used firewall software, warning that the flaw allows unauthenticated attackers to execute arbitrary code on unpatched appliances.

While the current version, 10.1, and three before it are not affected, the vuln, tracked as CVE-2021-3064, still exists in version 8.1.17 and all previous versions of PAN-OS, PAN's firewall operating system.

No exploit has yet been seen in the wild but exploitation is only a matter of time.

Action Point:

Update any affected products as soon as possible

'Critical Severity' Warning: Malware Found in Widely Deployed npm Packages

https://www.securityweek.com/critical-severity-warning-malware-found-widely-deployed-npm-packages

Software supply chain security jitters escalated again Friday with new "critical severity" warnings about malware embedded in two npm package managers widely used by some of the biggest names in tech.

According to separate advisories from GitHub, confirmed by the npm security team, two popular npm package managers -- the Coa parser and the rc configuration loader -- were compromised and rigged with password-stealing malware.

The rc package is widely distributed and used by major tech organizations and counts more than 14 million weekly downloads.

Action Point: The npm security team confirmed that the package rc had versions published with malicious code. Users of affected versions (1.2.9, 1.3.9, and 2.3.9) should downgrade to 1.2.8 as soon as possible and check their systems for suspicious activity.

"The npm package ua-parser-js had three versions published with malicious code. Users of affected versions (0.7.29, 0.8.0, 1.0.0) should upgrade as soon as possible and check their systems for suspicious activity," GitHub said.

Experts Analyze Proposed Bill Allowing Private Entities to 'Hack Back'

https://www.securityweek.com/experts-analyze-proposed-bill-allowing-private-entities-hack-back%E2%80%99

The 'hack back' controversy is like a well-rooted weed. No matter how often it is cut down, it always comes back. The latest iteration is a bi-partisan bill (S. 2292) introduced this summer that would require the DHS to weigh up the potential benefits and risks of allowing private entities to 'hack back'.

The idea persists because it is a form of self-defense – and the right to self-defense goes deep into the American psyche. The nation was founded as a form of self-defense against British imperialist tyranny; the right to bear arms continues the right of the people to defend themselves against any form of tyranny.

If the average American has the right to defend his home by striking back, why cannot he or she defend the network in a similar fashion? Since this is an emotional response to aggression, it will probably never go away.

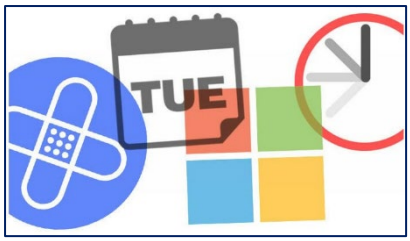
S. 2292 is cited as the "Study on Cyber-Attack Response Options Act". It was introduced on June 24, 2021 by senators Sheldon Whitehouse, D-R.I., and Steve Daines, R-Mont. Its purpose is to require the DHS to study and report on the risks and benefits of allowing private organizations to hack back at cyber aggressors, "subject to oversight and regulation by a designated Federal agency".

Action Point:

Updates on the progress of this legislation will be posted in Threatscape.

There is an additional potential risk with hacking back whereby the target may respond more robustly out of pique to counter-offensive activity, this is not an activity for the unprepared.

Rather than hacking back, says Ellis, "Organizations should perhaps focus instead on user awareness training, reducing their attack exposure, managing supply chain risk, proper segmentation, patching, Identity Access Management (IAM), and all the other things that make up a robust defense-in-depth program and that we frequently see fail."



Zero-Days Under Attack: Microsoft Plugs Exchange Server, Excel Holes

https://www.securityweek.com/zero-days-under-attack-microsoft-plugs-exchange-server-excel-holes

Microsoft on Tuesday pushed out patches for at least 55 documented security vulnerabilities in a wide range of products and called urgent attention to a pair of flaws that have already been exploited in the wild.

Microsoft said the two under-attack vulnerabilities exist in Microsoft Exchange Server and Microsoft Excel, two widely deployed products in the Windows ecosystem.

"We are aware of limited targeted attacks in the wild using one of vulnerabilities (CVE-2021-42321), which is a post-authentication vulnerability in Exchange 2016 and 2019," Redmond acknowledged, noting that the issue affects on-premises Microsoft Exchange Server, including servers used by customers in Exchange Hybrid mode.

Microsoft slapped a "critical" rating on the Exchange Server bug and warned that an authenticated attacker can launch code execution attacks. The company did not share details on the pre-patch attacks beyond crediting multiple Chinese researchers for the discovery.

The second zero-day was flagged in the popular Microsoft Excel productivity tool and is described as a "feature bypass vulnerability" that allows code execution via specially crafted spreadsheets. Microsoft said the Excel bug -- CVE-2021-42292 -- is being actively exploited but did not provide any additional details.

The Excel vulnerability affects Microsoft Office for macOS but patches for Apple's platform are not yet available.

Action Point:

"Our recommendation is to install these updates immediately to protect your environment," the company said.

Microsoft: Multiple Exchange Server Zero-Days Under Attack by Chinese Hacking Group | SecurityWeek.Com

---

Threat Actors are Exploiting Known Flaw in Zoho Password Management Service

https://view.email.sans.org/?qs=037604449b110927fd75112c94fb3c66b48eeb4ae055b7638a7894cf1623da2344079ddd09eb409b77edd8b3c9797ae31b19aec307708b09991a51053ff118004ab8208670167224

According to a report from Palo Alto Networks' Unit 42, threat actors have exploited a known vulnerability in Zoho ManageEngine AdSelfService Plus

to compromise networks at nine organizations in various sectors, including technology, defense, energy, and healthcare.

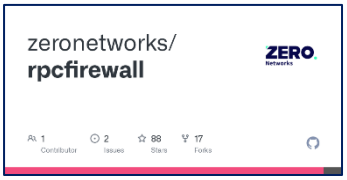
Read more in:
- unit42.paloaltonetworks.com: Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite Trojan and KdcSponge Stealer
- us-cert.cisa.gov: APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus
- thehill.com: Hackers breach nine global organizations in ongoing espionage campaign
- www.bleepingcomputer.com: State hackers breach defense, energy, healthcare orgs worldwide
- www.cyberscoop.com: Hackers with Chinese links breach defense, energy targets, including one in US
- www.govinfosecurity.com: NSA Reports: Espionage Group Breaches Critical Systems
- www.theregister.com: You'll never guess who's been exploiting the ManageEngine service to steal passwords.

The threat actors likely have ties to China. In mid-September, a US Cybersecurity and Infrastructure Security Agency (CISA) alert warned that the critical vulnerability was being actively exploited. Zoho has released updates to address the flaw.

Editor's Note
This flaw has been exploited since shortly after it was made public (and after a patch was released). Any vulnerable exposed system has likely been compromised. Palo Alto's blog lists some IOCs to watch out for, but there are likely other groups using this relatively easy to exploit vulnerability.

Action Point:

Reusable passwords are not only inherent unsecure, but they also require robust password reset processes since attackers have always targeted them. Self-service password reset software needs to be high security and ManageEngine did not live up to that. If you are using competing products for automated password reset, make sure you have applied all patches and chose a quality vendor.



RPC Firewall Dubbed 'Ransomware Kill Switch' Released to Open Source

https://www.securityweek.com/rpc-firewall-dubbed-ransomware-kill-switch-released-open-source

Today at Black Hat London, Zero Networks announced the release of its RPC firewall – also dubbed the 'ransomware kill switch' – into open source. The tool provides granular control over RPC, capable of blocking the use of lateral movement hacker tools and stopping almost all ransomware in its tracks.

Microsoft's Remote Procedure Call (MS-RPCE) lies at the heart of Windows. It effectively manages the relationship between clients and servers – if a client requests from a server, it goes through RPC; This happens both locally and between remote devices.

Over the last year, a relatively small number of ransomware gangs have been responsible for the majority of big game hunting ransom attacks:
Maze, Conti, REvil, Netwalker, DoppelPaymer, DarkSide and Avaddon. In every case--with the exception of Avaddon-- RPC has been used for reconnaissance and lateral movement.

The common hacker tools used for lateral movement – such as BloodHound, mimikatz, CobaltStrike, PS-Empire, PsExec and WMIC – all use RPC. But you cannot simply block the use of RPC. And even if you are able to detect something, detection is often too late.

To solve this problem and provide auditing, visibility and control over RPC calls, Zero Networks developed an agent that scans the machine and finds the RPC processes. “The agent hooks into those it finds in a legitimate manner (nothing malicious) so that it sees everything.,” Lakunishok told SecurityWeek.

“We provide full auditing and visibility so we can see, these are calling these RPC functions. Finally, we can map who is calling which RPC function. We can also create a whitelist. Even though RPC supports thousands of functions, only a few are really needed. We allow those and block everything else. We provide granular control over what RPC is doing. We can block the rest. Down the drain goes most of the attack tactics, and tools.”

The RPC Firewall will not stop all attacks. APT attackers will be able to find and use routes other than RPC – something tackled by Zero Networks’ commercial products. But the common lateral movement tools can be blocked, and network takeover stopped for all but the more advanced attackers.

Action Points and links:

Zero Networks has now open sourced this tool. It can be found on GitHub.

More importantly in today’s threat landscape, something like 86% of ransomware will be stopped in its tracks. “Ransomware is a bit simpler in the way it operates,” continued Lakunishok. “If you block just one of the things it uses, it simply doesn't move anymore.”

Related: NTLM Relay Attack Abuses Windows RPC Protocol Vulnerability

Related: Google Details How It Protects Data Within Its Infrastructure

Related: CrowdStrike Discloses Details of Recently Patched Windows NTLM Vulnerability

Related: Turla Cyber-Spies Target European Government With Multiple Backdoors

---

Kaspersky finds 31% increase in "smart" DDoS attacks

https://www.techrepublic.com/article/kaspersky-finds-31-increase-in-smart-ddos-attacks

The security company expects these attacks to keep rising through the end of the year.

Q3 beat every record in terms of daily number of DDoS attacks, according to a new report from Kaspersky. On August 18, Kaspersky observed 8,825 attacks, with more than 5,000 on both August 21 and 22. The total number of DDoS attacks was up 24% compared to Q3 2020 while the number of advanced, "smart" attacks was up 31% over the same time period.

Kaspersky defines a smart DDoS attack as one that is often targeted and used to disrupt services, make resources inaccessible or steal money.

Action Point:
Kaspersky experts offer these recommendations to strengthen defenses against these attacks:

- Maintain web resource operations by assigning specialists to respond to DDoS attacks.
- Validate third-party agreements and contact information, including those made with internet service providers.
- Establish typical traffic patterns and characteristics to make it easier to spot unusual activity related to a DDoS attack.
- Have a restrictive Plan B defensive posture ready to rapidly restore business-critical services during an attack.

2022 Cybersecurity Predictions from RSA Conference's Advisory Board

https://securityboulevard.com/2021/11/2022-cybersecurity-predictions-from-rsa-conferences-advisory-board/

A few notable predictions for the coming year from the RSA Advisory Board.

A Quest to Find Weaknesses in Systemic Dependencies:
Hugh Thompson, program committee chair, RSA Conference, said "it seems like there's a Jenga puzzle of society and dependencies that we have, yet we don't really know what it looks like until one of the pieces gets pulled." Inevitably, blocks will get removed in 2022. We need to think now about the impact each piece has on the whole puzzle to avoid seeing the tower come crumbling down.

Taking Ransomware to the IoT Level:
Caroline Wong, chief strategy officer at Cobalt predicted we will see malicious parties continue to scale and specialize when it comes to launching ransomware attacks. And yet, Wong said she expects to see some evolution in ransomware, particularly with regard to IoT.

The Skills Gap Will Escalate to Crisis Mode:
Skoudis predicted that "the lack of cybersecurity professionals and expertise will continue to grow to, essentially, a crisis mode as technology proliferates and gets more complicated and sophisticated. Cloud complexities and multi-cloud complexities are getting bafflingly difficult to deal with, and we don't have enough good people."

Action Point:

- As these predictions show we need to make sure that we are focused on threats targeting our supply chain, IoT and working to understand and mitigate the issues facing attraction and retention of cyber security personnel.

---

8 Best Practices for Data Security in Hybrid Environments

https://www.tripwire.com/state-of-security/security-data-protection/cloud/best-practices-for-data-security-in-hybrid-environments/

As more and more organizations are moving their sensitive data to the public cloud, the need to keep this data secure and private has increased significantly over time. Here are 8 Best practices outlined in the linked article.

1. Automate the Security Measures
Automating processes like coding the infrastructure and checking security compliance of the environment helps you to leverage your data security measures. Process automation allows you to keep track of your databases, and it notifies you about potential threats in real time.

2. Focus on High-level Data Encryption
Whether your data is at rest or in transit, always make sure that it is encrypted. Based on your specific requirements, undertake full-disk encryption, hardware encryption, and IPsec to keep your data protected in hybrid environments.

3. Train Your Employees in Security Practices
If an employee has access to your system and the data therein, it is essential to manage their permissions and to train them in operating the system in a secure manner.

4. Manage Data Throughout Its Lifecycle
From the moment datasets are created or imported into the system, you must undertake secure classification, compliance, and detection of potential threats.

5. Maintain Tight Control Over Data Access Rights
Always ensure that specific datasets are accessed only by the personnel who are authorized to do so. Implement multi-factor authentication to make sure that the right person is accessing the right data.

6. Pay Equal Attention to Cloud and On-Premises Portions of Your Environment
Always make sure that you have equal security controls for both cloud and on-premises portions of your hybrid environment.

7. Audit the Security Frameworks on A Regular Basis
It is advisable to get these frameworks audited at least once a year to ensure their efficiency and relevance.

8. Encrypt All Your Network Sessions

It is advisable for hybrid cloud users to encrypt every network session to protect their data in motion.

Action Point:

- Ensure that you address each of these 8 best practices across operational activities when moving data to cloud services and managing hybrid environments.

Don't underestimate the risk of an OT breach

https://www.helpnetsecurity.com/2021/11/10/underestimate-ot-breach/

A research study by Skybox Security found that 83% of organizations suffered an operational technology (OT) cybersecurity breach in the prior 36 months. The research unearths the uphill battle that OT security faces – comprised of network complexity, functional silos, supply chain risk, and limited vulnerability remediation options. Threat actors take advantage of these OT weaknesses in ways that don't just imperil individual companies – but threaten public health, safety, and the economy.

Forty-five percent of CISOs and CIOs say the inability to conduct path analysis across the environment to understand actual exposure is one of their top three security concerns. Further, CISOs and CIOs said disjointed architecture across OT and IT environments (48%) and the convergence of IT technologies (40%) are two of their top three greatest security risks.

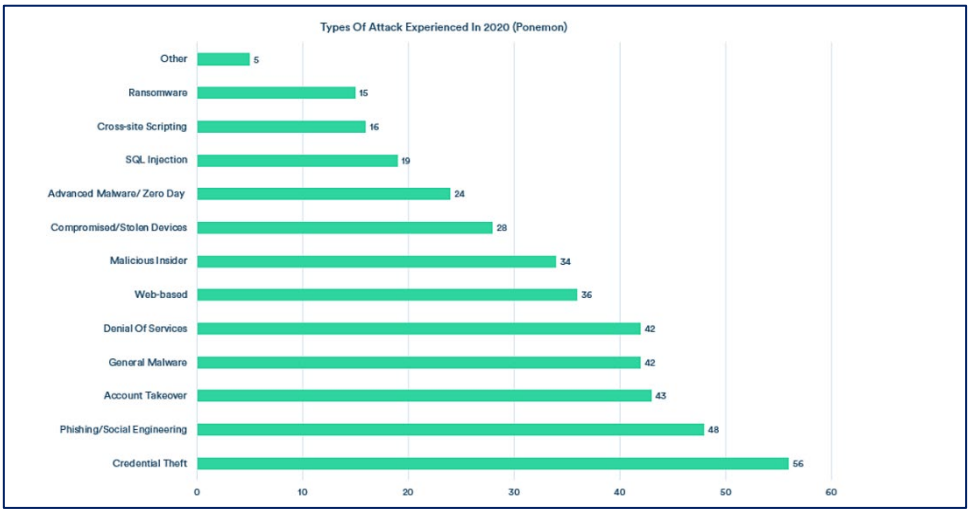
Forty percent of respondents said that supply chain/third-party access to the network is one of the top three highest security risks. Yet, only 46% said their organization as a third-party access policy that applied to OT.

Action Point:

- Understand the threat posed by IoT, vulnerabilities were up 46% versus the first half of 2020. This is a real threat to our operational models that needs to be addressed and OT brought into line with security thinking alongside IT.

Endpoint security

https://blogs.manageengine.com/desktop-mobile/desktopcentral/2021/11/09/7-features-key-to-a-unified-and-proactive-endpoint-security-solution.html



According to the 2020 Ponemon Institute report, 68% of organizations experienced one or more endpoint attacks in a span of 12 months that successfully compromised data and their IT infrastructure.

Attack surfaces at the endpoint level that need to be secured:

- Unauthorized plug-ins
- Unpatched applications/end of life applications/legacy software
- Malicious add-ons/browser extensions
- Unfiltered web URLs
- Malicious applications
- Absence of role-based privilege management
- Un-encrypted hard drive that poses a risk of data breach in case of hardware theft

56% of organisations faced credential theft and 28% of organisations faced attacks involving stolen devices and compromised devices. Some of the other types of attacks that target endpoints are ransomware, malware, zero-day, web- and browser-based, malicious insider, unauthorized devices, social engineering targeting malicious applications, and data theft from stolen devices.

Action Point:

- If we look at the types of attacks we are facing, the high impact ones involve ransomware but the most common involve the compromise and unauthorised use of accounts, a technique often used in many ransomware attacks. Deploy MFA as soon as possible.
- Endpoint security is more valuable than ever as a result of increased remote working. Look to invest in solutions that manage security controls and monitor for unusual and unwanted activities.

Recently released

	HEFESTIS Briefing Note – Credential stuffing prevention – CNIL enforcement
	Data Protection & Security 2021
	Cyber Attack Evolution 1
	Cyber Attack Evolution 2
	How to know you've been attacked
	How to respond to an attack
	Human Factor
	TTX Overview
	Ransomware Preparedness
	Supplier Security
	Breach Management Risks and Notification
	Data Protection by Design and Default
	Trusted Third Parties
	Data Breaches 1
	Data Breaches 2
	Ransomware preparedness checklist
	Acco unt Security Advisory
	Business Continuity Planning Webinar, presentation slides

	Business Continuity Planning Webinar, presentation recording
	Business Continuity Cheat Sheet
	BIA – HR System – Scotia University (template and example)
	Business Continuity Plan Template
	CRF 17. Business Continuity – HEFESTIS Breakdown

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Weekly Newsletter

In this week's threatscape we highlight endpoint security, the growing threat to Operational Technology, 2022 predictions from the RSA conference, increased DDoS activity and the latest vulnerabilities of concern.

Here are some of the week's Cyber Security articles which caught the attention of CISO-Share.

Sky fixes hijacking bug in 6m home broadband routers

https://www.theregister.com/2021/11/23/in_brief_security/

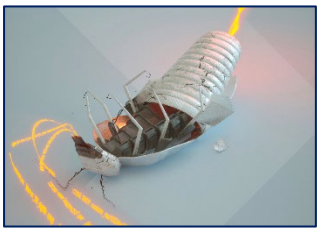
The vulnerability could be exploited by tricking a subscriber into viewing a malicious webpage. If an attack was successful, their router would fall under the attacker's control.

This exploitation is non-trivial and only works reliably if the subscriber hasn't changed their router username and password from the default of admin and sky.

Sky has released an update to address the issue.

Action Point:

- As there will be home workers using their Sky connections to access organisational data, issue like these show the need to protect home networking equipment as well. Advise users of the need to maintain equipment that they use to connect and change default passwords on home routers to further protect from compromise.



NCSC Annual Review 2021

https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021

The NCSC has released its annual review for 2021. This review looks at some of the key developments and highlights between 1 September 2020 and 31 August 2021. As part of a national security agency not all its work can be disclosed publicly but the review seeks to describe the year with insights and facts from colleagues inside and outside of the organisation.

The NCSC dealt with 777 incidents – an increase on last year – of which 20% were linked to the health sector and vaccines. They have engaged with around 5,000 organisations and issued guidance and threat assessments to 80 companies and 14 universities.

Action Point:

- Supply chain attack and ransomware are highlighted as continuing and growing threats. Ensure that you have protections and controls in place.
- They also have an overview of their incident management response model which may be of interest.
- Move over to the MyNCSC platform for managing the Active Cyber Defence programme.

New OWASP Top 10 for 2021

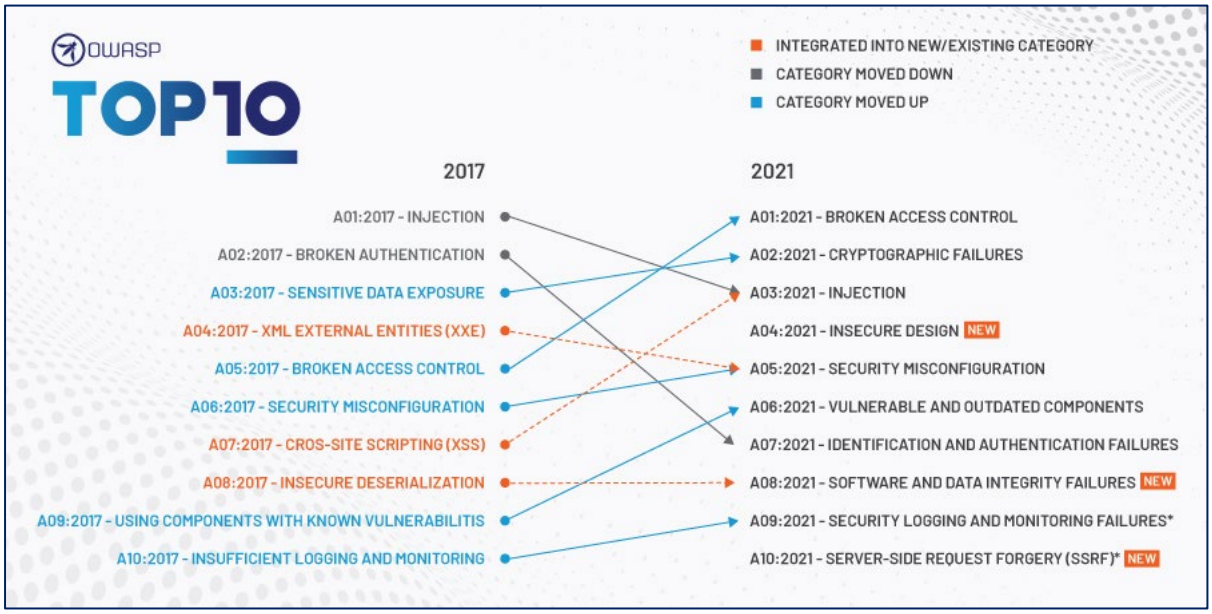
https://www.cyberlabs360.com/blog/new-owasp-top-10-for-2021-whats-new/

While the original OWASP Top 10 focused on vulnerability classification, the new list is more data driven and focuses on exploitability and impact.

A01-2021-Broken Access Control jumps to the Top of the List, a malicious user can access a function that should not be accessible to them. Elevation of privilege attacks and bypassing access control checks are good examples.

There are three new categories in the OWASP 2021 List. These include:

- A04:2021-Insecure Design
- A08:2021-Software & Data Integrity Failures
- A10:2021 -Server-Side Request Forgery (SSRF)



Action Point:

- Do regular pen testing in addition to automatic scans
- Refresh existing OWASP 10 training to align with the new OWASP 2021 list
- Consider using OWASP ASVS security framework and OWASP Proactive Controls which are more remediation focused

---

Draft IoT and smartphone security law

https://www.theregister.com/2021/11/25/product_security_telecoms_bill_parliament/

The Product Security and Telecommunications Infrastructure (PSTI) Bill is intended to drive up security standards in consumer tech gadgetry, ranging from IoT devices to phones, tablets, smart TVs, and so on.

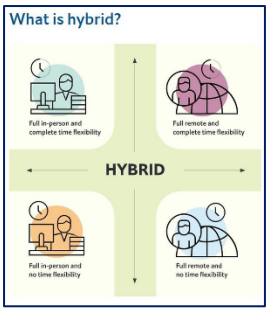
Digital infrastructure minister Julia Lopez MP said in a canned statement: "Our Bill will put a firewall around everyday tech from phones and thermostats to dishwashers, baby monitors and doorbells, and see huge fines for those who fall foul of tough new security standards."

This new cyber security regime will be overseen by a regulator, which will be designated once the Bill comes into force, and will have the power to fine companies for non-compliance up to £10 million or four per cent of their global turnover, as well as up to £20,000 a day in the case of an ongoing contravention."

A move like this would increase the security of consumer technology for all, including those that do not understand the importance or know how to secure technology devices themselves.

Action Point:

- If interested then the draft bill can be seen at: https://publications.parliament.uk/pa/bills/cbill/58-02/0199/210199.pdf



Hybrid work is here to stay. The new challenge is making sure it's not the worst of both worlds

https://www.techrepublic.com/article/hybrid-work-is-here-to-stay-the-new-challenge-is-making-sure-its-not-the-worst-of-both-worlds/

Research from Google Workspace finds that the next challenge is keeping both in-person and remote team members engaged.

The debate over all in-person vs. all remote work is mostly over and neither side won. Hybrid it is, according to two new surveys. New research from both Google Workspace and Kaspersky finds a lot of contradictions in how people are feeling about hybrid work. A significant group of workers like remote work but another chunk worries about how to network in that setting.

"Remote work does seem to result in better physical, social and mental well-being for me as an individual, but it does seem to come at the cost of connection to the organization," said Prasad Setty, vice president of digital work experience at Google Workspace.

The trade-off is worth it for some people as the Kaspersky research found that 61% of employees said they don't feel isolated while working remotely. Also, 37% of respondents said communication with colleagues is better now than before the pandemic.

Setty said the survey showed that only a small percentage of people expect to be fully in the office or fully remote.

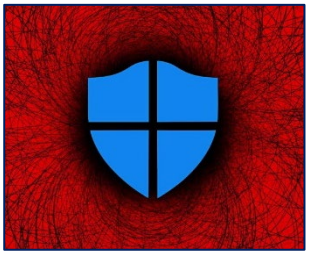
Action Point:
According to Google Workspace's research, "Making hybrid work human," attitudes have shifted enough so that the office is no longer the "natural" place for work to get done. The researchers identify reasons behind this shift:

- Some experiments with remote work will stick
- The tech set up is much better now in home offices
- Attitudes about remote work have shifted

People named the top three benefits of remote work as productivity, well-being and new ways of working, according to the research.

New Windows zero-day with public exploit lets you become an admin

https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/microsoft/new-windows-zero-day-with-public-exploit-lets-you-become-an-admin/amp/



A security researcher has publicly disclosed an exploit for a new Windows zero-day local privilege elevation vulnerability that gives admin privileges in Windows 10, Windows 11, and Windows Server.

BleepingComputer has tested the exploit and used it to open to command prompt with SYSTEM privileges from an account with only low-level 'Standard' privileges.

“We are aware of the disclosure and will do what is necessary to keep our customers safe and protected. An attacker using the methods described must already have access and the ability to run code on a target victim's machine.” – a Microsoft spokesperson.

Action Point:
"The best workaround available at the time of writing this is to wait Microsoft to release a security patch, due to the complexity of this vulnerability," explained Naceri.

As part of the November 2021 Patch Tuesday, Microsoft fixed a 'Windows Installer Elevation of Privilege Vulnerability' vulnerability tracked as CVE-2021-41379.

This vulnerability was discovered by security researcher Abdelhamid Naceri, who found a bypass to the patch and a more powerful new zero-day privilege elevation vulnerability after examining Microsoft's fix.

Yesterday, Naceri published a working proof-of-concept exploit for the new zero-day on GitHub, explaining that it works on all supported versions of Windows.

---

14 tactics to use during a ransomware negotiation

https://www.techrepublic.com/article/14-tactics-to-use-during-a-ransomware-negotiation/

Security researchers analysed 700 incidents to understand the economics of these threats as well as what bargaining tactics work.

Be polite during negotiations, ask for more time and always request a test file for decryption. Those are a few of the best practices for dealing with a ransomware attack, according to a new analysis of 700 incidents.

More about ransomware

- 10 ways ransomware attackers pressure you to pay the ransom

Pepijn Hack, cybersecurity analyst, Fox-IT, NCC Group and Zong-Yu Wu, threat analyst, Fox-IT, NCC Group wrote the research paper, "'We wait, because we know you.' Inside the ransomware negotiation economics." The researchers explain how adversaries use economic models to maximize profits and what strategies ransomware victims can use to win more time and reduce the final payment as much as possible. The report is based on two datasets. The first consists of 681 negotiations and was collected in 2019. The second dataset consists of 30 negotiations between the victim and the ransomware group and was collected from the end of 2020 and the first few months of 2021.

Learning Points:

Ransomware attackers are becoming increasingly organised

In addition to identifying helpful negotiation tactics, the researchers studied how attackers set the ransom figure. Each ransomware gang has created their own negotiation and pricing strategies meant to maximize their profits, according to the report. Also, many attackers spend weeks collecting data from the target's network, including sensitive data and financial statements. Adversaries know how much victims will end up paying, before the negotiations even start.

The researchers created an equation to predict the cost of a particular ransom. Elements of the equation include:

- The final ransomware demand on case
- The percentage left after exchanging the cryptocurrency to "clean" currencies
- The percentage left after paying the commission fee for the RaaS platform
- The final decision made by the victim on to pay or not, zero if the victim decided not to pay and one if the victim did pay
- The cost of carrying out the attack

GoDaddy Breach Exposes 1.2 Million Managed WordPress Customer Accounts

https://www.securityweek.com/godaddy-breach-exposes-12-million-managed-wordpress-customer-accounts

Domain registrar and web hosting giant GoDaddy has been hacked and customer data for some 1.2 million WordPress users were exposed to the attacker for more than three months.

The Tempe, Arizona-based GoDaddy disclosed the breach in an SEC filing and confirmed that millions of users of its managed WordPress hosting service had sensitive data stolen, including database usernames and passwords, email addresses and private SSL keys.

GoDaddy did not provide details on the compromise beyond a note that the attacker used a compromised password to access the provisioning system in its legacy code base for Managed WordPress.

The company said the hack began on September 6 and, over the last three months, the attacker gained access to valuable customer information.

Learning Points:

The raw details on the breach:

- Up to 1.2 million active and inactive Managed WordPress customers had email address and customer number exposed. The exposure of email addresses presents risk of phishing attacks.
- The original WordPress Admin password that was set at the time of provisioning was exposed. If those credentials were still in use, GoDaddy reset those passwords.
- For active customers, sFTP and database usernames and passwords were exposed. GoDaddy said it reset both passwords.
- For a subset of active customers, the SSL private key was exposed. GoDaddy says it is in the process of issuing and installing new certificates for those customers.

---

8 advanced threats Kaspersky predicts for 2022

https://www.techrepublic.com/article/8-advanced-threats-kaspersky-predicts-for-2022/

Advanced threats constantly evolve. This year saw multiple examples of advanced persistent threats under the spotlight, allowing Kaspersky to predict what threats might lead in the future.

Advanced persistent threats, which focus on cyberespionage goals, are a constant threat to companies, governments and freedom activists, to name a few. This activity keeps growing and evolving as more threat actors increase their skill.

Kaspersky released its advanced threat predictions for 2022 and shared interesting thoughts on next year's landscape. Here are eight advanced threats Kaspersky predicts will happen in the coming year.

Action Point:

This year has also seen many types of threats that rocked the cybersecurity community. There are also six 2021 threats articulated within this article which we have seen, according to Kaspersky.

Gartner top risks for 2022

https://www.helpnetsecurity.com/2021/11/15/2022-audit-plans/

Ransomware and the long-term effects of COVID-19 on markets and organisations are key items to cover in 2022, according to a Gartner report. The report also identified evolving societal expectations for enterprises, such as environmental, social and governance (ESG) risks, and operational resilience as top risk areas for 2022.

Action Point:

Recommend steps to provide assurance over organisational efforts to mitigate risk from ransomware attacks are:

- Evaluate employee security training
- Assess external relationships for ransomware support services
- Review ransomware attack response plans
- Assess data storage policies
- Review service provider ransomware attack communication protocols

---

Recently released

	HEFESTIS Briefing Note – Credential stuffing prevention – CNIL enforcement
	Data Protection & Security 2021
	Cyber Attack Evolution 1
	Cyber Attack Evolution 2
	How to know you've been attacked
	How to respond to an attack
	Human Factor
	TTX Overview

	Ransomware Preparedness
	Supplier Security
	Breach Management Risks and Notification
	Data Protection by Design and Default
	Trusted Third Parties
	Data Breaches 1
	Data Breaches 2
	Ransomware preparedness checklist
	Acco unt Security Advisory
	Business Continuity Planning Webinar, presentation slides
	Business Continuity Planning Webinar, presentation recording
	Business Continuity Cheat Sheet
	BIA – HR System – Scotia University (template and example)
	Business Continuity Plan Template
	CRF 17. Business Continuity – HEFESTIS Breakdown

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Weekly Newsletter

Good morning all and a warm welcome to this week's Threatscape where we highlight the security risks associated with staff burnout, guidance on securing organisational social media accounts, ways in which you could be inviting a cyber-attack and the Microsoft seizure of attacker domains.

Here are some of the week's Cyber Security articles which caught the attention of CISO-Share.

It's Not a User Problem; It's a Cybersecurity People Problem

https://securityboulevard.com/2021/12/its-not-a-user-problem-its-a-cybersecurity-people-problem/

The biggest cybersecurity threats all have one thing in common: Users.

One mistake shouldn't take down an entire network. The human problem can be seen as being enabled by cybersecurity people and leadership who fell short in their responsibilities. It's time to look at the user as just one part of the entire system.

"It's our responsibility in cybersecurity to look at all the enabling factors." For instance, the cybersecurity team should know why the user was in the system in the first place, how the user gained proximity to the incident and why the damage actually happened. Environment plays a big role in cybersecurity failures. More often than not, it is an issue within the network environment that ends up causing the user to do something wrong.

Action Point:

- Users should be taught to follow smart business practices and work within defined processes and procedures
- When investigating incidents make sure to learn how and why any user actions were permitted and how these can be addressed

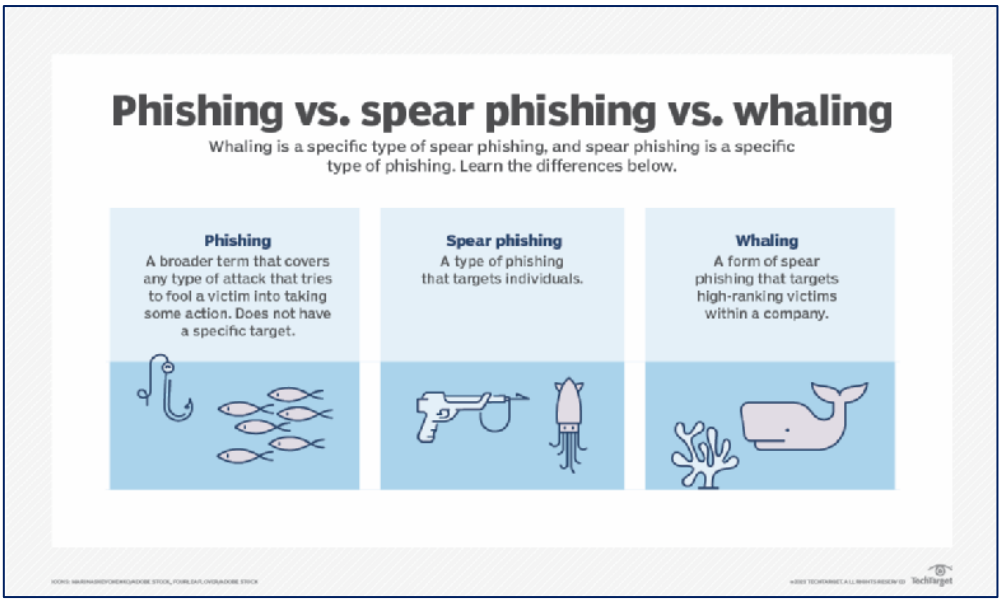
---

Top 11 email security best practices for 2022

https://www.techtarget.com/searchsecurity/tip/2019s-top-email-security-best-practices-for-employees

The article also gives a little information on the 11 best practices they have outlined below.

1. Train employees on email security best practices.
2. Create strong passwords.
3. Don't reuse passwords across accounts.
4. Consider not changing passwords regularly.
5. Use multifactor authentication (MFA).
6. Take phishing seriously.
7. Be wary of email attachments.
8. Don't click email links.
9. Don't use business email for personal use and vice versa.
10. Avoid public Wi-Fi.
11. Use email security protocols and tools. DKIM/SPF/DMARC.

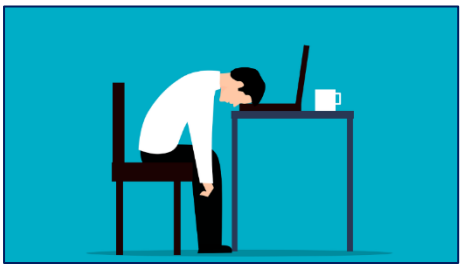


Action Point:

- Some useful information that can be used to inform and engage users on email best practice.

Burnout can lead to security threats, insider risk

https://www.securitymagazine.com/articles/96646-burnout-can-lead-to-security-threats-insider-risk



Burnout levels have risen throughout the COVID-19 pandemic. Employees in every industry are reporting burnout, which may lead to apathy and more security risks.
In response to this phenomenon, 1Password released its first State of Access benchmark report, "The Burnout Breach." The report, based on a survey of 2,500 adults, explores how workforce burnout has opened businesses to attacks

The report found that 84% of security professionals and 80% of other workers are feeling burned out, which has led to serious backsliding around security protocols. Burned out employees are a third less likely to follow their company's security guidelines (59% for burned out vs. 80% for not burned out).

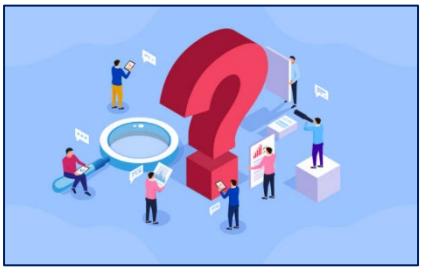
Burned-out employees are also 60% more likely than non-burned-out employees to create, download or use software and apps at work without IT's permission (48% vs. 30%.

Action Points:

- Engage and discover how people are using services and data for work
- Promote the behaviours and services that they should use to secure the institutions information
- Increase monitoring of unwanted behaviours, such as installing unauthorised applications or the use of personal cloud services
- To read more findings, view the full report https://1password.com/resources/2021-state-of-secure-access-report/

IT Risk Assessment: Is Your Plan Up to Scratch?

https://securityboulevard.com/2021/12/it-risk-assessment-is-your-plan-up-to-scratch/



IT risk assessment isn't just confined to cybersecurity. Hardware or software failure, backup and recovery problems, physical damage to devices or any other factor that could negatively affect IT infrastructure and disrupt business operations should be included.

The aim of a risk assessment is to identify weaknesses and loopholes in your organisation so that you can take remedial measures to close them before they become a bigger issue or are exploited by internal or external threat actors.

Risk assessment have many benefits including:

- Understanding your risk profile
- Evaluating existing security controls and tools

- Lower downtimes
- Help create robust policies
- Cost control
- Ensure compliance

Action Point:
Monitoring and managing risk is an ongoing process, risk needs to be an ongoing discussion and we recommend that it is formally introduced at the following points at a minimum.

- Regularly, at least once a year.
- Whenever there is a critical change in a policy requirement in order to remain compliant with the new laws and regulations.
- The occurrence of large-scale cybersecurity events has become commonplace.
- Change in internal business process.

CISA Releases Guidance on Protecting Organization-Run Social Media Accounts

https://www.cisa.gov/uscert/ncas/current-activity/2021/12/09/cisa-releases-guidance-protecting-organization-run-social-media

CISA has released Capacity Enhancement Guide (CEG): Social Media Account Protection, which details ways to protect the security of organization-run social media accounts.

CISA encourages social media account administrators to implement the protection measures described in CEG: Social Media Account Protection:

- Establish and maintain a social media policy
- Implement credential management
- Enforce multi-factor authentication (MFA)
- Manage account privacy settings
- Use trusted devices
- Vet third-party vendors
- Maintain situational awareness of cybersecurity threats
- Establish an incident response plan

Action Point:

- Requirements in the Scottish Governments Cyber Resilience Framework talk about the management of organisational social media accounts. This guidance from CISA can help us formally meet the needs of those requirements in an evidenced manner. Read more at the following link and integrate where necessary into existing or new control measures. https://www.cisa.gov/sites/default/files/publications/CISA_CEG_Social_Media_Account_Protection_508.pdf

- Further Capacity Enhancing Guides can be found at the following link and are also worth reading.
  https://www.cisa.gov/capacity-enhancement-guides-federal-agencies

---

What is Doxxing and How to Avoid It (UPDATED 2021)

Following a discussion with one of our members who have encountered this issue recently we include an informative article on Doxxing.

Doxxing is a type of cyber attack that involves discovering the real identity of an Internet user. The attacker then reveals that person's details so others can target them with malicious attacks. Doxxing is analyzing information posted online by the victim in order to identify and later harass that person.

Main Article

Support Article

What is doxxing?

The term "doxxing" comes from the expression "**dropping dox**", which was a revenge tactic used by hackers where they dropped malicious information on a rival.

Nowadays, doxxing is used to shame or punish people who would rather stay anonymous, because of their controversial beliefs or other types of non-mainstream activity.

Because most of us are careless with the information we share on the Internet, we tend to leave behind a trail of breadcrumbs a cybercriminal can use to find out our real identity, then deploy a string of malicious attacks.

This is called **doxxing**, and has messed up the lives of more than one person.

Action Point:

Everyone has some aspects of their lives that they would rather keep private. Those aspects may be harmless but they should remain private. They can range from hiding a surprise or a possibly insensitive comment from your spouse to keeping a political opinion from your coworkers and so on. Everyone has something they want to keep for themselves or share with a specific community.

Moreover, there are a lot of angry people on the internet who rely on doxxing to "win" an argument. **Any seemingly innocuous comment of yours has the potential to draw the anger of an internet mob.**

Avoid getting doxxed. Follow the steps outlined in this anti-doxxing guide to stay safe and anonymous.

SonicWall Urges Customers to Immediately Patch Critical SMA 100 Flaws

Network security vendor SonicWall is urging customers to update their SMA 100 series appliances to the latest version following the discovery of multiple security vulnerabilities that could be abused by a remote attacker to take complete control of an affected system.

Main Article

The flaws impact SMA 200, 210, 400, 410, and 500v products running versions 9.0.0.11-31sv and earlier, 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and earlier. The San Jose-based company credited security researchers Jake Baines (Rapid7) and Richard Warren (NCC Group) for discovering and reporting the shortcomings.

Action Point:

While there is no evidence that these vulnerabilities are being exploited in the wild, it's highly recommended that users move quickly to apply the patches in light of the fact that SonicWall devices have become a lucrative target for threat actors to launch a slew of malicious actions in recent months.

SolarWinds Hackers Use New Malware in Recent Attacks

The threat group believed to be responsible for the attack on IT management company SolarWinds has developed new malware as it continues to target organizations that possess data relevant to Russian interests.

Main Article

One year has passed since the discovery of the breach at SolarWinds and — despite their activities being analyzed and exposed by cybersecurity companies and researchers — the threat actor that launched the attack continues to target governments and private businesses, with their main goal apparently being the theft of data that could be useful to the Russian government.

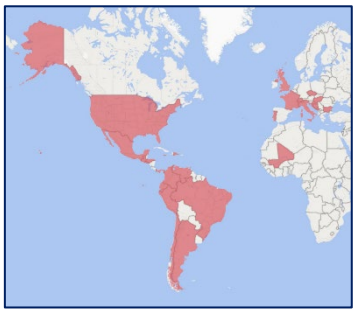
Incident response and threat intelligence firm Mandiant on Monday published a new report describing the threat group's most recent activities. The company tracks the threat actor and apparently related activity clusters as UNC2452, UNC3004 and UNC2652. Microsoft tracks the group as Nobelium, while others have linked the attacks to APT29 and Cozy Bear. There is wide consensus that the activity is conducted by a Russian intelligence agency.

Learning Point:

IoC's and more information are available from this article

Luke Jenkins noted that Microsoft currently tracks the malware as a variant of VaporRage, which the tech giant described in May. However, the expert has pointed out that while CEELOADER does share some similarities with VaporRage — they both function as a downloader for a second-stage encrypted payload — CEELOADER has junk code and other changes to make analysis more difficult. In addition, CEELOADER uses AES-256 to encrypt payloads, whereas VaporRage relies on a basic XOR algorithm.

Microsoft Seizes Domains Used by China-Linked APT 'Nickel'



Microsoft says it has seized control of domains that China-linked threat actor Nickel has been employing in malicious attacks targeting organizations in the United States and worldwide.

Main Article

The tech giant took over the websites after filing pleadings with the U.S. District Court for the Eastern District of Virginia, which quickly granted an order in this regard.

While the move will prevent the group's access to some of its victims, it is unlikely to put an end to Nickel's activities. However, Microsoft does believe that the infrastructure it just seized was used as part of the group's most recent wave of attacks.

"Obtaining control of the malicious websites and redirecting traffic from those sites to Microsoft's secure servers will help us protect existing and future victims while learning more about Nickel's activities," Microsoft says.

Learning and Action Points:

In activity Microsoft has been tracking since 2019, Nickel has been using the **now seized** websites to execute attacks on victims in a total of 29 countries in Europe, Central and South America, the Caribbean, and North America, mostly for harvesting intelligence from government agencies, human rights organizations, and think tanks.

IoC's and recommended actions are available from this Microsoft link

---

8 Ways You Could Be Inviting a Cybersecurity Attack

Cultural and systemic issues may be leaving your organization vulnerable.

Main Article

Many business leaders still believe cybersecurity is a problem that can be solved if they invest enough money and hire the right people with the right technical knowledge who will keep them out of the headlines.

In fact, it's often systemic and cultural issues between IT and non-IT executives, not technical competency or funding, that leave organizations exposed to cybersecurity attacks.

Learning Point:

The cost of recovery and the resulting downtime in the aftermath of a ransomware attack, as well as the reputational damage, can be 10 to 15 times more than the ransom.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

From: CISO Shared Service - UCSS <CISO-SHARE@JISCMAIL.AC.UK> **On Behalf Of** David Robertson
Sent: 03 December 2021 08:36
To: CISO-SHARE@JISCMAIL.AC.UK
Subject: David Robertson shared "HEFESTIS Weekly Newsletter" with you.

[CAUTION]This email originated from outside of the College - do not click links or attachments unless you recognise the sender and know the content is safe. If you have any concerns please contact ICT at ictservicedesk@glasgowkelvin.ac.uk.

Microsoft SharePoint

CISO Share

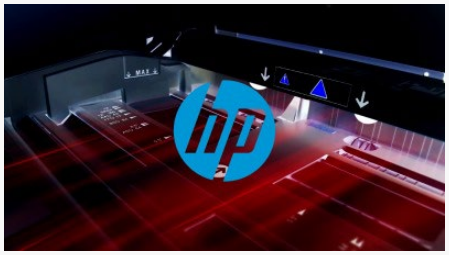
HEFESTIS Weekly Newsletter

A very warm welcome to all of you from all of us at HEFESTIS
In this week's Threatscape we highlight the changes to the Cyber Essentials scheme which come into effect in January 2022. The changes, as articulated on the IASME web site, may pose significant challenges, especially to larger institutions and represent a much higher level of compliance for digital estates, especially in relation to cloud-based environments. Patching, cyber-insurance, phishing and ransomware also feature in this week's issue.
Please check the CiSP site, as always, for the latest updates on the incident and countermeasures to protect your institution.
Here are a few of the articles which caught the attention of the CISO-Share team this week.

IASME CONSORTIUM

THE JANUARY CHANGES TO THE CYBER ESSENTIALS SCHEME ARE HIGHLY SIGNIFICANT

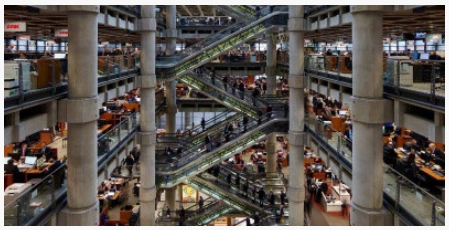
The Government approved Cyber Essentials scheme includes five technical controls that help protect organisations from the majority of cyber attacks. Main Article A team of experts review the scheme at regular intervals to ensure it stays effective i...
David Robertson
12/1/2021



Critical Vulnerability Found in More Than 150 HP Printer Models

Multiple Vulnerabilities Found in More Than 150 HP Printer Models; Critical Flaw Could Allow Attackers to Move Laterally Main Article Support Article The exposed port vulnerabilities are classified as CVE-2021-39237 (critical severity), and the font...

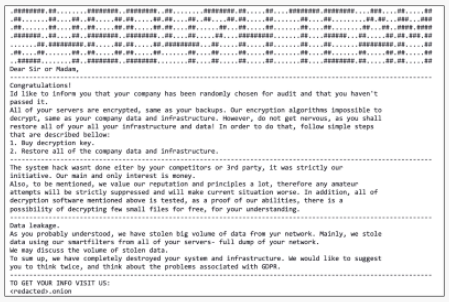
David Robertson
12/2/2021



Lloyd's Carves Out Cyber-Insurance Exclusions for State-Sponsored Attacks

The insurer won't pay for 'acts of cyber-war' or nation-state retaliation attacks. Main Article Fallout from nation-state sponsored cyberattacks will no longer be covered under cyber-insurance policies issued by famed insurer Lloyd's of London. The ...

David Robertson
12/2/2021



Dear Sir or Madam,

Congratulations!
Id like to inform you that your company has been randomly chosen for audit and that you haven't passed it.
All of your servers are encrypted, same as your backups. Our encryption algorithms impossible to decrypt, same as your company data and infrastructure. However, do not get nervous, as you shall restore all of your all your infrastructure and data! In order to do that, follow simple steps that are described bellow:
1. Buy decryption key.
2. Restore all of the company data and infrastructure.

The system hack wasnt done eiter by your competitors or 3rd party, it was strictly our initiative. Our main and only interest is money.
Also, to be mentioned, we value our reputation and principles a lot, therefore any amateur attempts will be strictly suppressed and will make current situation worse. In addition, all of decryption software mentioned above is tested, as a proof of our abilities, there is a possibility of decrypting few small files for free, for your understanding.

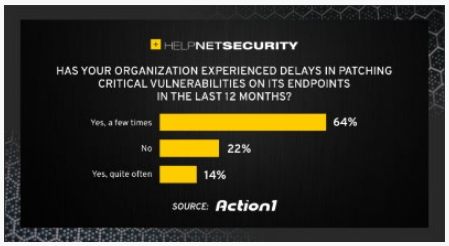
Data leakage.
As you probably understood, we have stolen big volume of data from yur network. Mainly, we stole data using our smartfilters from all of your servers- full dump of your network.
We may discuss the volume of stolen data.
To sum up, we have completely destroyed your system and infrastructure. We would like to suggest you to think twice, and think about the problems associated with GDPR.

TO GET YOUR INFO VISIT US:
<redacted>.onion

54BB47H - 'Sabbath' Ransomware Operators Target Critical Infrastructure

Since June 2021, a relatively new ransomware group called Sabbath has been targeting critical infrastructure in the United States and Canada, including education, health and natural resources. Main Article According to a warning from Mandiant, the g...

David Robertson
12/1/2021



Patching takes 2.5 times longer when endpoints are remote

Action1 released a report based on the feedback from 491 IT professionals worldwide. The study explores how organizations patch and manage their remote and office-based endpoints and provide employees with remote IT support. Some of the issues iden...

Steve McIntosh
11/30/2021

Vulcan advisors share patch management best practices

Vulcan Cyber advisors Brian Lozada, CISO at HBOMax, and Steve Zalewski, former deputy CISO of Levi Strauss, provide their thoughts on some of the challenges of patch management in an evolving cyber security landscape. Main Article Some of their comm...

David Robertson
12/2/2021

Project Zero Flags High-Risk Zoom Security Flaw

Video conferencing software giant Zoom has shipped patches for a pair of security defects that expose Windows, macOS, Linux, iOS and Android users to malicious hacker attacks. Main Article The flaws, discovered and reported by Google Project Zero re...

David Robertson
11/30/2021

Phishing Remains the Most Common Cause of Data Breaches

Data from Dark Reading's latest Strategic Security Survey shows that more companies experienced a data breach over the past year because of phishing than any other cause. The percentage of organizations reporting a phishing-related breach is slightl...

Steve McIntosh
12/1/2021

Secure cloud products and services with new CIS Benchmarks

CIS followed the lead of the Cloud Service Providers (CSP), and grouped services by CSP product. Each CSP offers dozens of products, grouping cloud services based on the function they provide. The Beginner's Guide to Secure Cloud Configurations des...

Steve McIntosh
12/1/2021

AI is changing everything about cybersecurity, for better and for worse. Here's what you need to know

Artificial intelligence and machine learning tools could go a long way to helping to fight cybercrime. Following recent warnings from the head of MI6 (see support article) we include this informative piece from earlier in the year courtesy of ZDNet....

David Robertson
12/2/2021

Go To Site

Get the SharePoint Mobile App

To unsubscribe from the CISO-SHARE list, click the following link:
https://www.jiscmail.ac.uk/cgi-bin/WA-JISC.exe?SUBED1=CISO-SHARE&A=1

From: CISO Shared Service - UCSS <CISO-SHARE@JISCMAIL.AC.UK> **On Behalf Of** David Robertson
Sent: 17 December 2021 11:00
To: CISO-SHARE@JISCMAIL.AC.UK
Subject: Threatscape

[CAUTION]This email originated from outside of the College - do not click links or attachments unless you recognise the sender and know the content is safe. If you have any concerns please contact ICT at ictservicedesk@glasgowkelvin.ac.uk.

A very warm welcome to all of you from all of us at HEFESTIS. Whilst we offer our hopes and wishes for a wonderful festive break we have dedicated our communications this week to what is a singularly pernicious, pervasive and incalculably widespread threat – Log4J.

This week's Threatscape magazine has been replaced by circulation of a briefing paper relating to the Log4J vulnerability which is being treated as a clear and present risk facing our institutions and supply chains at a global level. I would like to thank all of our members for their participation in yesterdays seminar on this subject. It was great to hear that we are all heading in the same direction in facing this threat. There is a section of hints, tips and tools shared by the attendees which is included within the briefing paper. Updates will be posted on our SharePoint site on an ongoing basis.

Although we have little information whilst awaiting an imminent CREW notice, it has been reported that ArcGIS has been added to the growing list of vulnerable services which may be affected.

Please check the CiSP site, as always, for the latest updates on the incident and countermeasures to protect your institution.

If you have any questions or comments please feel free to contact us.

Kind regards

David

David Robertson
M: 07852 330122
E: drobertson@hefestis.ac.uk

Darren Clement
M: 07442 859979
E: dclement@hefestis.ac.uk

Steve McIntosh
M: 07904 908945
E: smcintosh@hefestis.ac.uk

HEFESTIS

2021

Log4J Briefing Paper

BRIEFING

DAVID L ROBERTSON

HEFESTIS | HIGHER EDUCATION/FURTHER EDUCATION SHARED TECHNOLOGY AND INFORMATION SERVICES STIRLING BUSINESS CENTRE, WELLGREEN, STIRLING, FK8 2DZ

Contents

Log4J Briefing 3
Threat/Risk profile 3
The threat is already evolving 3
Impact 3
Identification and remediation may take time 4
It's important to prioritise external and internet-facing applications over internal applications due to their internet exposure, although both are vulnerable 4
Mitigation 4
Short term: Secure perimeter defences, practice disaster recovery and protect back ups 4
Long term: Patch and Move to zero trust, security by design, security in depth models 4
Recommendations over the festive break. 4
Hints, tips, tools and links from our membership 6
A tool to mitigate Log4Shell in old versions of Java by disabling log4j JNDI 6

Log4J Briefing

The widely used Log4j logging tool is affected by a critical remote code execution vulnerability that has been increasingly exploited by malicious actors, including profit-driven cybercriminals and state-sponsored groups.

The vulnerability is tracked as CVE-2021-44228 and it has been dubbed **Log4Shell** and LogJam. The vulnerability is being actively and increasingly exploited by cyber-criminals and is evolving with new variants being reported daily.

Threat/Risk profile

It's safe to say this vulnerability will have, and already is having, a massive effect globally.

Log4j is used by thousands of applications, libraries, and frameworks, meaning the number of potentially impacted organisations is staggering. And with attackers already scanning the internet to find vulnerable targets, if organisations haven't already started taking mitigation steps, then it may already be too late.

The way modern products are built is using a big hierarchy of dependencies, where developers use libraries written by third-party companies and engineers to speed up the software release process. Log4J is an extremely basic library that allows log writing in Java applications. The way CVE-2021-44228 affects comes in 3 layers - cloud products that directly use the Log4J, web applications that use libraries that use Log4J, and off-the-shelf software which is internally deployed on customer servers and endpoints making this vulnerability deeply pervasive with complex dependencies for mitigation.

As fixing, changing and deploying cloud applications can be fast, updating libraries that use Log4J can break functionality unless done with caution. As of right now, only 114 of 17170 libraries which use Log4J are actually safe (0.66%). *Source – TechRepublic. The most problematic fixes are internally deployed software, which will have to wait for a vendor update or a security patch, in that scenario customers are advised to wait on further vendor guidance and as of right now are potentially helpless in reacting.

Directly mitigating the vulnerability involves update of the log4j package itself and not just Java. There was an early misconception, that updating Java could reduce the severity of the vulnerability, which is simply no longer considered to be sufficient.

If an organisation uses log4j or software that includes the library, then it's safest to assume breach is of a high likelihood and review potentially impacted applications for odd behaviour. Furthermore, if already breached then remove all physical network access to the affected server/environment.

The threat is already evolving

When a vulnerability is discovered and makes as much noise as Log4Shell, it invariably signals that there are additional vulnerabilities in the same software or fixes for that software and triggers additional research and discovery. In this case, the initial fix provided was developed in a way that mitigated the exploitable symptom but didn't properly address the root cause.

This also highlights the dangerous dependency on open-source libraries which power large portions of the Internet but are ultimately written and maintained by unfunded volunteers with limited available time. It is unlikely that this will be the last exploit of this nature to be discovered. This also means that even up to date, fully patched environments with the latest security fixes installed may well still be vulnerable to this type of attack.

Impact

The log4j vulnerability has created endless golden opportunities for bad actors – and they know it and are getting creative. What they're trying to do now is build an arsenal of tools that they can use across the globe for theft and service disruption, especially ahead of the holiday season.

DDoS attacks in particular are a top concern, as exploitation could allow bad actors to download, install and then fully control an army of botnets. DDoS operators can then focus on attacks that bring down critical infrastructure ahead of the holiday season, a time when people are notoriously distracted, tired and more prone to making security mistakes – with the added option for follow on disruption and infiltration by threat actors against compromised systems and digital estates.

Risk scoring 100% – threat level highest, impact level highest, likelihood imminent

Identification and remediation may take time

Right now, every IT person in the world is trying to identify if their machines have vulnerable Log4j packages. Attackers are winning because combatting unexpected major zero-day vulnerabilities like Log4Shell takes an incredible amount of time—and time-to-patch—particularly in large enterprises. And time is often the determining factor for the amount of damage from a breach.

To guard against Log4j, IT teams need to assess where they need to look for vulnerabilities, what machines need to be patched, and what software needs to be updated to protect against attackers. To minimise further damage while large-scale patching efforts are being made, we advise security teams to explore platforms/services that allow them to rapidly search their enterprise assets for software that may include the vulnerable Log4j packages.

According to Mike Wiacek, Founder and CEO, Stairwell: One approach could include searching across file metadata such as file paths and file names or hashes. Another approach could include scanning enterprise file content with customised YARA rules to identify files and artifacts associated with log4j components. These types of searches can accelerate otherwise slow and laborious defensive processes and further help organisations assess where related software exists, where it is out of date, where it is vulnerable, and where to look for post-exploit activity should an attacker make a move before patching can occur.

Priority

It's important to prioritise external and internet-facing applications over internal applications due to their internet exposure, although both are vulnerable.
On balance external scanning and exploitation activity and threat levels are currently generating a considerably greater risk profile than that associated with insider activity.

Mitigation

Short term: Secure perimeter defences, practice disaster recovery and protect back ups
The exploit, like many others, relies on a call-home step to a command-and-control (C2) server.

To prevent these kinds of attacks, organisations should restrict egress (outbound) connectivity. Each subnet, server and workload should be allowed to connect only to the endpoints that are required by business. All other destinations should be blocked.

Blocking egress connections is easy with standard security controls such as firewalls, but defining the policy, which egress connections are allowed, is tough. Doing this properly requires continuous learning of legitimate application connectivity patterns, and enforcement in production environments.

Ensure you have a secure restore position and practiced procedures in place to recover your digital estate in the event of a significant breach.

Long term: Patch and Move to zero trust, security by design, security in depth models
The vulnerability highlights that applications often blindly use libraries without careful consideration of all available options. *Including maintaining a repository of libraries that are deemed secure as part of a secure DevOps process and as part of the fundamental IT security strategy with defined security standards.

Recommendations over the festive break.
Safety first – if possible all potentially affected services – especially external/web based services should be considered at risk.

Consider shutting down anything that's not confirmed OK and set a default "deny" for any outbound traffic.

Consider restricting staff/student access to IT services to monitored, on prem only with no non-essential external access over the festive period.

Resources and Advisory: NVD - CVE-2021-44228 (nist.gov).

We have compiled a list of tools and other resources that can be useful for defenders concerned about the impact of the Log4Shell vulnerability which may be of assistance – however there is an (over) abundance of advice and information being released in relation to Log4J vulnerability.

Following the alerts from NCSC, CRU< JiSC and numerous further sources it has been established that the Log4j2 open source logging framework for Java is subject to a vulnerability which means untrusted input can result, via LDAP, RMI and other JNDI endpoints, in the loading and executing of arbitrary code from an untrusted source.

Cloudflare are saying they first saw exploitation on: 2021-12-01 04:36:50 UTC. That suggests it was in the wild at least 9 days before publicly disclosed but some time after it was disclosed to Apache.

We recommend that a co-ordinated mitigation response be applied to all and any organisations exposed to this vulnerability. In cases whereby existing vulnerability procedures are providing challenge, it may be considered appropriate to co-ordinate mitigation more in line with incident response procedures and plans.

Generic incident response plan templates are available from our SharePoint site here

And included within this embedded document Incident Response Process Template.doc

Resources: We have collated some resources available from our SharePoint site and these links:

The NCSC is advising organisations to take steps to mitigate the Apache Log4j 2 vulnerability.

The main NCSC page is available here

Additional information links - with thanks also to our members in Robert Gordon University and Dundee and Angus College for sharing this info:

Main Article

Symantec Info

Techrepublic Update

Infographic and information from Swiss Government

https://blog.cloudflare.com/actual-cve-2021-44228-payloads-captured-in-the-wild/

https://www.lunasec.io/docs/blog/log4j-zero-day/

https://www.vmware.com/security/advisories/VMSA-2021-0028.html

Microsoft article, Defender already has signature for these: https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

Possible vendors affected: https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

Thread with a lot of info: https://www.reddit.com/r/blueteamsec/comments/rd38z9/log4j_0day_being_exploited/

List of potential IOC: https://research.nccgroup.com/2021/12/12/log4shell-reconnaissance-and-post-exploitation-network-detection/

Nessus plugins: https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability

Some exploitation proof: https://github.com/YfryTchsGD/Log4jAttackSurface

Hints, tips, tools and links from our membership

- For those of you using Nessus, they recommend and update the following template https://www.tenable.com/plugins/nessus/156061
- Incident response plans can be based on this framework and playbooks, https://www.gov.scot/publications/cyber-resilience-incident-management/
- This list of vendors is being updated regularly
- https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592
- https://status.salesforce.com/generalmessages/826 some information about Tableau
- Useful site from the dutch ncsc - log4shell/software at main · NCSC-NL/log4shell (github.com)
- Guardicore which deploys agents on servers to manage the local firewalls etc, and to give central logging may help in augmenting Nessus scans.
- List of IOCs - https://github.com/NCSC-NL/log4shell/blob/main/iocs/README.md
- log4shell/README.md at main · NCSC-NL/log4shell
- Operational information regarding the vulnerability in the Log4j logging library. - log4shell/README.md at main · NCSC-NL/log4shell
- We've been scanning filesystems looking for vulnerable classfiles using https://github.com/fox-it/log4j-finder
- Some people have PDQ https://www.pdq.com/blog/log4j-vulnerability-cve-2021-44228/
- Ran the PDQ (post above) scan which picked up most servers with Log4j 2.x.x versions. Then ran this script which identified a further V2 server and also the V1 servers.

  ```
  $Log4jFiles = Get-ChildItem -path "C:\" -file "log4j*.jar" -Recurse -ErrorAction SilentlyContinue foreach ($jarfile in $Log4jFiles) { [PSCustomObject]@{ 'Filename' = $jarfile.Name 'Location' = $jarfile.FullName 'Sha1Hash' = (Get-FileHash $jarfile.FullName -Algorithm SHA1).hash }
  ```

A tool to mitigate Log4Shell in old versions of Java by disabling log4j JNDI
Full support details and article here

Research NCC group are releasing **log4j-jndi-be-gone**, a dead simple **Java agent** that disables the log4j JNDI handler outright. It also supports Java 6 through 17, covering older versions of log4j that support Java 6 (2.0-2.3) and 7 (2.4-2.12.1), and works on read-only filesystems (once installed or mounted) such as in read-only containers.

Update (12/16/21): Due to the way it works, log4j-jndi-be-gone will prevent any JNDI lookups, including Thread Context Map-based ones that still impact log4j 2.15.0, but it does not prevent the limited "denial-of-service" attack against that version under such configurations.

The benefit of this Java agent is that a single command line flag can negate the vulnerability regardless of which version of log4j is in use, so long as it isn't obfuscated (e.g. with proguard), in which case you may not be in a good position to update it anyway. log4j-jndi-be-gone is not a replacement for the -Dlog4j2.formatMsgNoLookups=true system property in supported versions, but helps to deal with those older versions that don't support it.

Using it is pretty simple, just add -javaagent:path/to/log4j-jndi-be-gone-1.0.0-standalone.jar to your Java commands. In addition to disabling the JNDI handling, it also prints a message indicating that a log4j JNDI attempt was made with a simple sanitization applied to the URL string to prevent it from becoming a propagation vector. It also "resolves" any JNDI format strings to "(log4j jndi disabled)" making the attempts a bit more grep-able.

```
$ java -javaagent:log4j-jndi-be-gone-1.0.0.jar -jar myapp.jar
```

log4j-jndi-be-gone is available from our GitHub repo, https://github.com/nccgroup/log4j-jndi-be-gone. You can grab a pre-compiled log4j-jndi-be-gone agent JAR from the releases page, or build one yourself with **./gradlew**, assuming you have a recent version of Java installed.

From: David Robertson <DRobertson@hefestis.ac.uk>
Sent: 14 January 2022 18:02
To: CISO-SHARE@JISCMAIL.AC.UK; HEIDS-INFOSEC@JISCMAIL.AC.UK <HEIDS-INFOSEC@JISCMAIL.AC.UK>; SCIL@JISCMAIL.AC.UK; DPO <dpo@hefestis.ac.uk>; hwcert@hw.ac.uk <hwcert@hw.ac.uk>
Subject: Threatscape Newsletter

[CAUTION]This email originated from outside of the College - do not click links or attachments unless you recognise the sender and know the content is safe. If you have any concerns please contact ICT at ictservicedesk@glasgowkelvin.ac.uk.

Good afternoon everyone and a belated but warm welcome to 2022 to all of you from all of us at HEFESTIS.

We start out with the best news first - we have had no reported Log4J or other significant incidents amongst our membership over the traditional Christmas and New Year break. We congratulate you all for the preparations made to ensure the integrity of your digital estates over what is the time of year most likely to generate and experience a cyber-attack, when available support is low and threat actors are most active. Great job.

This week we cover the latest Microsoft security patching, with some vulnerabilities already identified. We not only look back at 2021 but also forward to trends in 2022.

Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments please feel free to contact us.

Kind regards
David

David Robertson
M: 07852 330122
E: drobertson@hefestis.ac.uk

Steve McIntosh
M: 07904 908945
E: smcintosh@hefestis.ac.uk

Darren Clement
M: 07442 859979
E: dclement@hefestis.ac.uk

David Lowe-Robertson
Chief Information Security Officer
HEFESTIS North Region
P: 07852 330122
E: drobertson@hefestis.ac.uk
hefestis.ac.uk

Higher Education/Further Education Shared Technology and Information Services
Stirling Business Centre, Wellgreen, Stirling, FK8 2DZ

HEFESTIS is an active promoter of sustainable behaviours and would ask any visitors to the premises to consider the environment. All offices are conveniently located in close proximity to mainline train stations and coffee/tea and water will be provided at meetings. HEFESTIS has a voluntary ban on bringing single use drinks bottles / single use coffee cups into their offices and to their events, visitors are discouraged also from bringing in such single-use products to HEFESTIS's offices and events. Please don't print this email unless you really need to.

HEFESTIS Ltd is co-owned by member institutions across the Scottish University and Colleges sectors, Incorporated in Scotland SC603511

CONFIDENTIALITY NOTICE
This email is intended only for the addressee named above. As this email may contain confidential or privileged information, if you are not the named addressee or the person responsible for delivering the message to the named addressee, please telephone us immediately on 0131 442 8930. The contents should not be disclosed to any other person nor copies taken. We do not accept any liability or responsibility for: (1) changes made to this email after it was sent, or (2) viruses transmitted through this email or any attachment.

HEFESTIS Weekly Newsletter

Good morning everyone and a belated but warm welcome to 2022 to all of you from all of us at HEFESTIS.

We start out with the best news first - we have had no reported Log4J or other significant incidents amongst our membership over the traditional Christmas and New Year break. We congratulate you all for the preparations made to ensure the integrity of your digital estates over what is the time of year most likely to generate and experience a cyber-attack, when available support is low and threat actors are most active. Great job.

This week we cover the latest Microsoft security patching, with some vulnerabilities already identified. We not only look back at 2021 but also forward to trends in 2022.

Please check the CiSP site, as always, for the latest updates on current incidents and countermeasures to protect your institution.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

List of data breaches and cyber attacks in December 2021 – 219 million records breached

2021 was a difficult year many of us, and with the hope that COVID-19 will dissipate in the spring, this is a new year more than any other where we want to look forwards, not backwards.

But before we turn our attention to 2022, we must first round out 2021 with our final monthly review of data breaches and cyber attacks. December saw 74 publicly disclosed security incidents, which accounted for 219,310,808 breached records.

Main Article

You can find the full list of incidents in the main article, with those affecting UK-based organisations listed in bold.

Review of 2021

Log4J

Phishing scams

Learning Points: Additional Information

- Double extortion ransomware victims soar 935%
- Russian man sentenced for providing 'bulletproof hosting' for cyber criminals
- Microsoft seizes control of websites used by China-backed hackers

---

Microsoft January 2022 Patch Tuesday: Six zero-days, over 90 vulnerabilities fixed

This month's round of security fixes includes patches for publicly-known remote code execution bugs.

Main Article

Microsoft has released 96 security fixes including updates to address six zero-day vulnerabilities.

In the Redmond giant's latest round of patches, usually released on the second Tuesday of each month in what is known as Patch Tuesday, Microsoft has fixed problems including remote code execution (RCE) exploits, privilege escalation flaws, spoofing issues, and cross-site scripting (XSS) vulnerabilities.

SECURITY

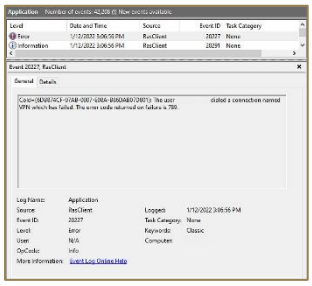
- NoReboot attack fakes iOS phone shutdown to spy on you
- JFrog researchers find JNDI vulnerability in H2 database consoles similar to Log4Shell
- Cybersecurity training isn't working. And hacking attacks are getting worse
- The 5 best VPN services in 2022
- The biggest data breaches, hacks of 2021

Products impacted by January 2022's security update include Microsoft Exchange Server, the Office software line, Windows Defender, Windows Kernel, RDP, Cryptographic Services, Windows Certificate, and Microsoft Teams.

Action Points:
The zero-day vulnerabilities resolved in this update are:

- **CVE-2021-22947**: HackerOne assigned CVE: An open source Curl RCE allowing for Man-in-The-Middle (MiTM) attacks.
- **CVE-2021-36976**: MITRE assigned CVE: An open source Libarchive use-after-free bug leading to RCE.
- **CVE-2022-21874**: A local Windows Security Center API RCE vulnerability (CVSS 7.8).
- **CVE-2022-21919**: A Windows User Profile Service Elevation of Privilege security issue (CVSS 7.0), PoC exploit code recorded.
- **CVE-2022-21839**: Windows Event Tracing Discretionary Access Control List Denial-of-Service (DoS) (CVSS 6.1).
- **CVE-2022-21836**: Windows Certificate spoofing, PoC code recorded (CVSS 7.8).

None of the zero-day flaws above are known to have been exploited in the wild. A total of 24 vulnerabilities were patched earlier this month in Microsoft Edge (Chromium-based). According to the Zero Day Initiative (ZDI), this volume is unusual for the month of January, with previous years often being roughly half this number.



On 11th January, Microsoft released Windows updates to fix security vulnerabilities and bugs as part of the January 2022 Patch Tuesday

We are getting multiple reports of issues with the latest security patch, and a concern raised from one of our members. Here are early links to the issues currently identified - mainly from blog resources which may help inform the decision as to when and where to apply this latest security update.

Link article 1 Link article 2 Link article 3

Action Points:

- Many Windows admins also report on Reddit that the bug also affects connections to SonicWall, Cisco Meraki, and WatchGuard Firewalls, with the latter's client also affected by the bug.
- With many users still working remotely, admins have been forced to remove the KB5009566 and KB5009543 updates, which immediately fixes the L2TP VPN connections on reboot.
- Windows users can remove the KB5009566 and KB5009543 updates using the following commands from an Elevated Command Prompt.
- As Microsoft bundles all security updates in a single Windows cumulative update, removing the update will remove all fixes for vulnerabilities patched during the January Patch Tuesday.
- Therefore, Windows admins need to weigh the risks of unpatched vulnerabilities versus the disruption caused by the inability to connect to VPN connections.
- It is not clear what caused the bug, but Microsoft's January Patch Tuesday fixed numerous vulnerabilities in the Windows Internet Key Exchange (IKE) protocol (CVE-2022-21843, CVE-2022-21890, CVE-2022-21883, CVE-2022-21889, CVE-2022-21848, and CVE-2022-21849) and in the Windows Remote Access Connection Manager (CVE-2022-21914 and CVE-2022-21885) that could be causing the problems.
- Unfortunately, there is no known fix or workaround for the L2TP VPN connection issues at this time.

U.S. Government Issues Warning Over Commercial Surveillance Tools

The U.S. State Department and the National Counterintelligence and Security Center (NCSC) on Friday issued a warning over the use of commercial surveillance tools.

Main Article

The one-page document says governments and other entities have been using spyware sold by companies and individuals. The spyware can typically be used to record audio, track a device's location, and access all of the content stored on a phone.

"Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections. In some cases, malign actors can infect a targeted device with no action from the device owner. In others, they can use an infected link to gain access to a device," the alert reads.

The alert also includes some general recommendations for mitigating "some risks" posed by surveillance tools. However, the government warned that "it's always safest to behave as if the device is compromised."

- **Learning Point:** While the document does not name any specific spyware, it likely refers to the infamous tools made by the controversial Israel-based NSO Group.

Apache Foundation Calls Out Open-Source Leechers

The Apache Software Foundation (ASF) is calling out for-profit companies leeching on open-source code, warning that "only a tiny percentage" of downstream vendors are contributing to securing the open-source ecosystem.

Main Article

"[The] community is defined by those who show up and do the work. Companies that build open source into their products rarely participate in their continued maintenance," the ASF said in a position paper published ahead of a high-level White House meeting on open-source software security.

"Only a tiny percentage of downstream companies (reusing the same code within their own products) choose to participate [in maintaining the code]," the Foundation said, noting that any future directives must "avoid placing additional unfunded burdens on the few maintainers who are already doing the work."

Learning Points:

"While part of the solution may be to ensure companies know what they've included in their supply chain, they will also need to have processes for rapidly handling and disclosing vulnerabilities in their dependencies. Users of open source software also need to keep track of lifecycles and ensure the projects they are using are still getting security updates," it added.

"We can't fix open source supply chain issues by focusing exclusively on the upstream producer," the group warned, noting that even perfect software releases can take years to be adopted and deployed by downstream providers.

Cyber Command announces partnership with 84 universities

U.S. Cyber Command announced it will partner with 84 universities across 34 states this year as part of a program to build up the nation's cybersecurity workforces.

Main Article

The Academic Engagement Network represents an opportunity for the Department of Defense and other agencies as they have struggled to recruit and retain top cybersecurity talent. Something that we can all relate to.

Learning Points:
We can look to our own and other HE/FE sector programmes to recruit, and develop new talent.

---

10 Lessons Learned from the Top Cyber Threats of 2021

10 Lessons Learned from the Top Cyber Threats of 2021

This article details the top 10 lessons learnt from the biggest vulnerabilities and incidents of 2021.

Main Article

Microsoft Exchange Server Vulnerabilities

1. Continuously check your network traffic for anomalies

2. Perform threat hunting after patching

DarkSide Ransomware Campaign

3. Practice risk management for the worst case event

4. Implement behaviour-based detection

Kaseya MSP Supply Chain Attack

5. Adopt a zero trust strategy

6. Monitor use of built-in operating system utilities

Atlassian Confluence Remote Code Execution Vulnerability

7. Maintain strict supervision of your public-facing applications

8. Test the effectiveness of your security controls

Apache Log4j Vulnerabilities

9. Improve visibility of your software inventory

10. Better utilize security controls.

Action Points:

- To learn more and see further details follow the link to the site.
- Consider these lessons learned and how your organisation can adopt these measures to reduce the threat.

Issues for Consideration Going Into 2022

Main Article

Better communication with the board

The three ways this could be improved are:

- a structured governance model with high level representation
- an agreed set of KPIs that reflect business requirements and
- regular opportunities to demonstrate how security is a business enabler.

Ensuring security is resilient to business change

This can be achieved by planning for business continuity/disaster recovery activities ahead of time and sharing ownership of them. Table Top eXercises are also crucial in this regard.

Risk should be a problem shared

There is a strong need to identify several risk owners in the business and not simply delegate it to IT.

Prepping for "The Great Resignation"

Remote working is a potential solution; distributed teams are seen as a necessity in some circumstances but there is also certainly a need to get teams to meet face-to-face on a regular basis.

Keeping IT out of the shadows

Solving shadow IT challenges starts with usability, preventing risky workarounds by removing the obstacles that invite them.

Light at the end of the tunnel for third party risk management?

There is some work being done to produce frameworks that ensure a standardized attestation for third parties but we need to ensure their scope is broad enough to include any vendor or employee that has remote login access to any enterprise applications. That includes any subcontractors that may work for the contractor, as credential-sharing is common across companies.

More focus on data and privacy

The Schrems judgement requires us to take greater focus on data and where it is stored. Also verifying user identity, checking the health of all user devices, and securing access to any application is key.

Managing security debt

The need to manage older systems while adapting to the new environment and the risk and cost that this incurs is especially important to consider in the operational technology (OT) area. We need to track and address security debt, organizations must develop and implement defined, repeatable processes. They should look to strategies like the zero-trust model, trust but verify, sanitation of inputs and outputs, and of course, make sure to execute patches instead of pushing it onto the next person.

Ransomware, ransomware, ransomware

A main tactical issue of concern, this form of attack is of greater concern to those with unmanaged or legacy systems. There are plenty useful guides out there to prepare and respond to ransomware attacks. Including the HEFESTIS preparedness document.

Action Points:

- Consider the points raised in this article and how they can be discussed internally at your organisation.
- Ensure that you have taken the steps to protect your organisation from ransomware.

9 ways that cybersecurity may change in 2022

As malicious bot activity increases and attacks surge against APIs, MFA will become more of a mandate and the CISO will take on a greater role, predicts Ping Identity CEO and founder Andre Durand.

Main Article

The dramatic rise in ransomware and other cyberattacks over the past year has finally driven home the point that cybersecurity needs to be taken much more seriously. Amid initiatives by the U.S. government and other parties, there's a growing global awareness of the need to focus on security to combat attacks that threaten vital areas of society. How might this renewed focus on security start to play out in 2022? Ping Identity CEO and founder Andre Durand offers his take with nine cybersecurity predictions for the new year.

Learning Points:

Cybersecurity will become an ESG issue

ESG (environment, social and governance) is a method used by investors and other people to evaluate businesses based on more socially conscious standards. With greater investments in security needed to protect society, cybersecurity will become the fourth responsibility of ESG for corporations, according to Durand.

- MFA will become a global mandate
- Bad bot tsunami
- Focus will shift to Zero Trust authorization
- Rise of digital wallets
- Attacks on zombie and shadow APIs
- Convergence of IT and OT
- Identity focus shifts to user experience
- Rise of the CISO

SecurityWeek Cyber Insights 2022: Ransomware

Ransomware has grown from humble beginnings as threat-based scams to a worldwide criminal phenomenon. It has been a continuous process of extortion refinement, with criminals adapting their behavior to maximize their financial return. This evolutionary process will continue.

Main Article

Increasing extortion

The purpose of ransomware is financial extortion. The intent is extortion – encryption-based ransomware is merely a successful methodology. This methodology will be abandoned or adapted without a thought if some better method of extorting money is found, or if the current method no longer provides an adequate return.

For now, the criminals are content with refining their approach to extortion and maximizing their return from it.

Action Points:

- We cannot eliminate bad actors and we cannot prevent hacking. The only way to stop the scourge of ransomware/extortion is to make it less attractive to the attackers. This would require industry to stop paying ransoms – either by choice or by lack of necessity – or for law enforcement to prevent payments reaching the attackers.
- Stopping ransomware will require the cooperative action of law enforcement, legislation, the security industry and the commercial targets. Law enforcement and governments will need to make it harder for extortion gangs to receive payment. The security industry needs to make security controls more effective and easier to implement. CI and manufacturing need to develop better physical resilience, while commercial organizations need to better protect their sensitive data.
- "We aren't even close to being better protected," comments Mark Guntrip, senior director for cybersecurity strategy at Menlo Security. "For ransomware to stop, business continuity and disaster recovery strategies need to improve to a point where enterprises can sustain the attack and have the right tools. Only then will we see the cost of ransomware go down. These tools don't exist yet."
- The aim must be to make extortion so difficult and costly for the attackers that they simply move on to easier pickings. Frankly, we are nowhere near achieving this – meaning that extortion is still in the growth phase of its lifecycle. For this reason alone, we can say with confidence that there will be more extortion with increasing demands throughout 2022.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

Glasgow Kelvin College

Risk Management Committee

Minute

Meeting held on Tuesday 2 November 2021 at 2pm online using Microsoft Teams

Item	Action Agreed	Member	Target Date
1	**Sederunt**		
	L Clark, Director of Corporate Services (Chair); G Lawson, Health and Safety Manager; I Gordon, Head of Facilities and Environmental Sustainability; J Gallagher, Quality Enhancement Development Manager; L Lang, Communications and Marketing Manager; M McKerlie, Head of Services to Support Learners; R MacKenzie, Senior Administration Officer; and J Carroll (recording purposes only).		
2	**Apologies**		
	D Smeall, Principal; J Evans, Vice Principal Operations; A McGhee, Director of Business Development; D Shiels, Director of Human Resources; and P Brown, Director of Planning, Performance and Curriculum.		
3	**Terms of Reference**		
	L Clark highlighted that she would liaise with the Director of Human Resources regarding Equality representation.	**LC**	
	L Clark confirmed that the meeting was quorate with 7 members in attendance.		
	Members noted the content of the Terms of Reference for information purposes.		
4	**Draft Minute of Previous Meeting held on 24 August 2021**		
	The minute was accepted as a true and accurate record of the business conducted at the previous meeting.		

Item	Action Agreed	Member	Target Date
5	**Matters Arising from the Minutes of the Previous Meeting**		
	Item 9b: Data Protection Impact Assessment (DPIA)		
	L Clark reminded members that Data Protection Impact Assessments (DPIA) were living documents which required to be monitored by project leads in conjunction with members of the data protection team during the lifetime of any Data Sharing Agreement (DSA) between the College and any organisation.		
	Item 8: GDPR/Cyber Security		
	L Clark would liaise with the Director of Digital Services regarding the following matters identified at the Cyber Security Audit: • Introduction to Phishing Training: including simulation test that measured staff Cyber Security awareness; • Logging/Intrusion Detection; and • Mandatory Cyber security module.	**LC**	
	Item 12aii: Risk Appetite and Risk Register Review:		
	Risk Category: Statute and Regulations		
	The Health and Safety Manager reported that volunteers had been recruited and were currently participating in First Aid training.		
	M McKerlie reported that there was a First Aid incident at Easterhouse Campus where a First Aider could not attend. The Health and Safety Manager was keen that this situation did not reoccur and hoped further volunteers could be recruited in the near future.		
	There was still a requirement for volunteer Fire Wardens with liaison ongoing between the Director of Human Resources and Trade Unions.	**GL/DSH**	
	Risk Category: Human Resource Management – High Absence Rates due to poor Mental Health		
	Review to be considered prior to December 2021 Board meeting: L Clark would liaise with J Evans and D Shiels.	**LC/JE/ DS**	
6	**Health and Safety**		
a)	**Health and Safety Annual Report**		
	G Lawson reported that the Health and Safety Annual Report had been approved by the Board of Management.		

Item	Action Agreed	Member	Target Date
	Members noted the content of the Health and Safety Annual Report for information purposes.		
	b) Health and Safety Minutes: 9 June 2021		
	G Lawson took members through the content of the Health and Safety Minutes including: • Health and Safety training: Managing Safely, Occupational Health and Wellbeing; • FLU Jab: the college was looking for another provider to participate in FLU Voucher Programme who had an adequate number of stores within the Glasgow area. • Health and Safety underspent went on project including Support for Learning equipment, Trauma kits and gritting equipment at West Campus. Members noted the content of the Health and Safety Minutes for information purposes.		
7	**Finance**		
	There were no Finance matters for discussion.		
8	**GDPR/Cyber Security**		
	a) ICT Penetration Test Conducted		
	L Clark reported excellent feedback from the ICT Penetration Test conducted by Barrier Networks following the report presented at a meeting of SMT by Andy Laszlo. There were no major areas of concern with only minor tweaks to be actioned.		
	b) Asset Management/News Articles from City of Glasgow		
	Referring to articles that had appeared in the local press and media regarding the theft of £0.5m worth of laptops from City College of Glasgow, L Clark reported that the college already had systems and procedures in place to prevent this type of risk to college business. A Fixed Asset Management process was in place, while orders of more than £250 per item or multiple orders would, necessarily, require the scrutiny and approval of the Procurement Manager. Notwithstanding, the Fixed Asset Procedure would be reviewed and enhanced where necessary.	**LC**	
	Members noted the content of the news articles for information purposes.		

Item	Action Agreed	Member	Target Date
c)	**Consultation UK - Plans to Depart from GDPR**		
	R MacKenzie reported on the UK Government consultation "Data: a new direction" on plans to depart from the current UK GDPR which, the Government argued, would enhance UK business innovation. Proposals under consideration include: • Data Protection Officer: no mandatory requirement to appoint a DPO; • No mandatory requirement for Data Protection Impact Assessments; • Scrapping of the need to maintain a Record of Processing Activities (ROPA); • Charging for Subject Access Requests to be re-introduced; • Changes to thresholds for reporting Data Breaches; • Reform of the Information Commissioner's Office (ICO).		
	While the proposals presented significant changes to GDPR and the current data protection arrangements, it was noted that UK Data Privacy and legal experts also feared that the proposals posed a threat to citizen's civil liberties and data privacy rights which could endanger the UK's 'Adequacy' decision which was vital for the unencumbered free transfer of data between the EU and UK.		
	L Clark confirmed that the College would submit a response to the Consultation before the 19 December 2021 deadline. The outcome of the consultation would be reported back to this Committee in due course.	**LC/ RMcK**	
d)	**Data Share Agreement: Review Schedule**		
	Members noted the content of the Data Share Agreement Review Schedule for information purposes.		
e)	**Data Retention Schedule**		
	L Clark reminded members that liaison was ongoing with ICT regarding recommendations for discussion threads within Microsoft Teams, which should be restricted to a maximum 3-month duration due to the impact from Subject Access Requests (SARs).	**LC**	
	Following a considerable discussion, members decided:		
	• Microsoft Teams data retention should be discussed at SMT; and	**LC**	
	• Report and Support required to be added to the Data Retention Schedule.	**LC**	

Item	Action Agreed	Member	Target Date
	f) Henderson Loggie: Internal Audit Annual Plan 2021/22		
	L Clark reported that some specific dates for the Internal Audit Plan 2021/22 had still to be confirmed. However, Internal Audit would begin the process in December 2021 with Quality Assurance and Student Support.		
	Members noted the content of the Internal Audit Annual Plan for information purposes.		
	g) ICO: Accountability Framework		
	R McKenzie spoke to the content of the ICO Accountability Framework. The Framework represented a new approach to ensuring data protection compliance while providing standardisation of reporting across the sector.		
	L Clark advised that the College would liaise with the College Data Protection Officer to produce the new Framework. A report on the new Framework would be considered at the Audit and Risk Committee.		
	Members noted the content of the Framework for information purposes.		
9	**Insurance**		
	a) Domestic/International Travel Advice		
	L Clark reported concerns regarding financial risks arising from insurance for domestic and international travel.		
	Following considerable discussion, it was agreed that current travel advice needed to be revised and that a robust process was required. L Clark would liaise with the Procurement Officer to discuss an online system and procedure to track and record domestic and international travel which would include the Clarity Booking System.	**LC**	**TBA**
	b) Insurance Cover 2021-22 - NOT IN THE PUBLIC DOMAIN -		
	L Clark reported that the cost of insurance for Cyber Security had doubled.		
	Members noted the content of the Insurance document for information purposes.		

Item	Action Agreed	Member	Target Date
10	**Estates**		
a)	**Estates Capital Report for GCRB** I Gordon requested members to note the content of the Estates Capital Report for GCRB for information purposes that was on track to achieve spending requirements by March 2022.		
b)	**Estates Update: October 2021** I Gordon spoke to the content of the Estates Update that sought to provide information regarding progress regarding improvements in the college estate. Members noted the content of the Estates Update for information purposes.		
c)	**Walking Route between Springburn Campus and Springburn Railway Station: Feasibility Report March 2019** L Clark reported that consultation was now taking place with SPT regarding the possibility of a walking route from Springburn Campus to the Railway Station, which had support from the Principal regarding funding. Following discussion, it was noted that the project may not go ahead due to the ancillary costs of SPT upgrading the Railway Station to meet accessibility standards. L Clark informed members that she would report feedback to this Committee. Members noted the content of the Feasibility Report for information purposes.	**LC**	
d)	**High Energy Prices** Responding to concerns about the global hike in the cost of gas and electricity, I Gordon reported that the College currently benefitted from a fixed tariff until April 2022. However, thereafter, the College would experience a significant increase in the energy costs which would have a significant impact on the College's budget. L Clark and I Gordon would monitor the matter closely.	**LC**	

Item	Action Agreed	Member	Target Date
11	**Human Resources**		
a)	**Report and Support**		
	L Clark informed members that the Report and Support initiative provided learners and staff with the opportunity to report any concerns about inappropriate behaviour and to access support information.		
	L Clark reported that Report and Support had been included in the Privacy Notice. R McKenzie confirmed that the Report and Support DPIA would be reviewed within six months.		
	An update on Report and Support would feature at the Audit and Risk Committee.		
12	**Risk Management Update**		
	L Clark reported that the Risk Register was in the process of being revamped through Zurich Insurance and would be presented at the next meeting.	**LC**	
	She took members through the content of the Risk Management Update that included the following information: • planned Risk Management Training Sessions; • the potential impact on the College of any theft on the scale of that experienced at City of Glasgow College; and • COP26: activities and possible disruption to college business from travel and activist arrangements.		
	Following discussion regarding transport arrangements during COP26, it was decided that L Clark and I Gordon would discuss this matter outwith today's meeting.	**LC/IG**	
	Members noted the content of the Risk Update for information purposes.		
13	**Items for Information**		
	G Lawson reminded members that the law on fire alarms was changing for domestic premises regarding interlinked fire alarms requiring to be installed by February 2022 and he sent the relevant link to members for information purposes.		

a) HEFESTIS Newsletters from 27 August 2021 to 22 October 2021

R McKenzie summarised the content of the HEFESTIS Newsletters including:

- Cybercrime on the increase including cases of hackers contacting employees to steer cyber-attacks.

Members noted the content of the HEFESTIS Newsletters for information purposes.

b) Audit Scotland Publications

L Clark reported that the Audit Scotland Publications had been considered by the Audit and Risk Committee.

Members noted the content of the Audit Scotland Publications for information purposes.

14 Equality Management - Issues to be considered as a consequence of the consideration of the above

Members agreed that no further Equality Management issues were raised as a consequence of the meeting.

15 Risk Management - Issues to be considered as a consequence of the consideration of the above

Members agreed that the following new Risk Management issues were raised as a consequence of the meeting:

- First Aid not being available when needed; **GL**
- Fire Wardens urgently required; **GL**
- COP26 Event: possible impact on college business. **ALL**
- Financial risks arising from:
  - insurance regarding domestic and international travel; and **LC**
  - future energy price increases. **LC**

16 Data Protection – Issues to be considered as a consequence of the consideration of the above

Members agreed that cyber risks remained high and acknowledged the success of the ICT Penetration Test.

17 Closure

L Clark thanked members for their attendance and contributions to the meeting. The meeting closed at 2:55pm.

18 Date of Next Meeting

Tuesday 25 January 2022 at 2pm via Microsoft Teams.