Cyber Security Update

Simon Bulleyment

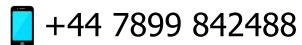
Director





www.sibrossa.com









Key trends

- Ransomware
- Social engineering
- Evolving state threats
 - Russia, China, North Korea, Iran
- Digital supply chain attacks
 - SolarWinds, Log4j
- Attack points
 - Backup systems, remote access systems, weak passwords, unpatched systems





Ransomware — what's changed?

- How it was
 - WannaCry (2017)
- 'Professionalisation' of ransomware organisations
- Ransomware as a Service
 - Shift from sophisticated to the less sophisticated
- Double extortion tactics
 - Data exfiltration
- Multi extortion tactics
 - Denial of Service (DoS) attacks
- Recent notable incidents
 - Ireland's Health Service Executive (Conti), UK education sector (Ryuk)
 - 2021 20% of incidents NCSC handled targeted at health/vaccine orgs





Ransomware in 2022



66%

hit by ransomware in the last year



65%

72%

attacks resulted in data encryption



experienced an increase in volume/ complexity/impact of cyber attacks



\$812,360

average ransom payment (excluding outliers)



86%

ransomware attack caused loss of business/revenue

SOPHOS Cybersecurity delivered.

The State of Ransomware 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries.



98%

pay-out rate on ransomware claims





Social engineering attacks

- Targeted phishing attacks
- The rise of smishing
- Microsoft Threat Intelligence Center (Aug 2022)
 - SEABORGIUM
 - Primarily targets NATO countries, particularly US/UK
 - Source of attacks ... guess who?!
 - Use of social media, LinkedIn, general open-source intelligence
 - Attacks on Microsoft 365 (email: attachments/URLs, OneDrive)
- What can you do?
 - Review email security controls
 - User awareness and processes
 - Implement multi-factor authentication (MFA)





SEABORGIUM

	RA @outlook.com> 4:37 A Increasing cybersecurity.
	If there are problems with how this message is displayed, click here to view it in a web browser.
	Dear colleagues,
) shared the paper. Did you get it?	In the context of growing tension in the international community and an increase in the number of active hacker groups operating in the information field, we are recording attempts by unidentified persons to attack the information infrastructure of our institute.
Cheers,	First of all, we cooperate with information security experts to increase the level of security of our resources.
From: Sent: To: @outlook.com> Subject: Re: Wondering what you guys think	At the same time, do not forget about the personal training of each employee. For your safety and informational awareness, we have prepared analytical material for possible review. International Cyber-Activity.pdf (reading time 13 min.)
Please send the attachment	We hope that by joint efforts we will achieve significant success in the security of our institute.
Get Outlook for iOS From: @outlook.com> Sent: Tuesday, June 8, 2021 8:53:41 AM To: Subject: Re: Wondering what you guys think	Sincerely,
Subject. Ne. Frondering what you gays think	

know you have your hands full at the moment, but nevertheless thought this would interest you (attached).





Where can you get help?

- National Cyber Security Centre guidance
- For smaller organisations, cyber security guides
 - Small Charity Guide https://www.ncsc.gov.uk/collection/charity/cyber-security-small-charity-guide-pdf-download
 - Small Business Guide https://www.ncsc.gov.uk/collection/small-business-guide
- For medium and larger organisations, 10 Steps to Cyber Security
 - https://www.ncsc.gov.uk/news/large-uk-organisation-10-steps-stay-ahead
- For larger organisations, the cyber security Board Toolkit
 - https://www.ncsc.gov.uk/collection/board-toolkit





What can you do?

- Update risk assessments
 - https://www.ncsc.gov.uk/collection/risk-management-collection
- Cyber improvement plan/strategy
- Implement controls, <u>review effectiveness</u>, <u>test</u>
- Cyber insurance
- Cyber incident response plan
 - Consider a third-party service
 - Table-top exercises
 - Red Team testing
- NCSC Early Warning Service
 - https://www.ncsc.gov.uk/information/early-warning-service





Cyber Essentials

- Government backed
 - Aim
- Value to organisations
- What is is
 - Self assessment
 - Covers five areas
 - Annual renewal
 - Fixed fee
 - Prescriptive controls
- It's difficult to achieve ... and that's a good thing!
- Cyber Essentials Plus



Micro organisations (0-9 employees)	£300 +VAT
Small organisations (10-49 employees)	£400 +VAT
Medium organisations (50-249 employees)	£450 +VAT
Large organisations (250+ employees)	£500 +VAT

