


• Cyber Security Update

Simon Bulleyment

Director

 sbulleyment@sibrossa.com 

www.sibrossa.com 

 +44 7899 842488



Certified Information
Systems Security Professional





Topics

- Ransomware
- Targeted phishing attacks
- What you can do and where you can get help
- Cyber Essentials



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



Ransomware in 2022



66%
hit by ransomware in the last year



65%
attacks resulted in data encryption



72%
experienced an increase in volume/
complexity/impact of cyber attacks



46%
paid the
ransom



61%
encrypted data
restored after
paying the
ransom

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.



\$812,360
average ransom payment
[excluding outliers]



86%
ransomware attack caused
loss of business/revenue



83%
have cyber insurance
against ransomware

98%
pay-out rate on ransomware claims



Phishing attacks

- Phishing/spear phishing
- The rise of smishing attacks
- Microsoft Threat Intelligence Center
 - SEABORGIUM
 - Primarily targets NATO countries, particularly US/UK
 - No prizes for guessing origin of attacks!
 - 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



[Redacted]@outlook.com> | [Redacted]

4:37 AM

Increasing cybersecurity.

i If there are problems with how this message is displayed, click here to view it in a web browser.

Dear colleagues,

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.

First of all, we cooperate with information security experts to increase the level of security of our resources.

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.)

We hope that by joint efforts we will achieve significant success in the security of our institute.

Sincerely,

[Redacted signature]

I shared the paper. Did you get it?

Cheers,
[Redacted]

From: [Redacted]
Sent: [Redacted]
To: [Redacted]@outlook.com>
Subject: Re: Wondering what you guys think

Please send the attachment

Get [Outlook for iOS](#)

From: [Redacted]@outlook.com>
Sent: Tuesday, June 8, 2021 8:53:41 AM
To: [Redacted]
Subject: Re: Wondering what you guys think

[Redacted]

I 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
- Cyber Security: Small Charity Guide
 - <https://www.ncsc.gov.uk/collection/charity/cyber-security-small-charity-guide-pdf-download>
- For larger charities, the cyber security Board Toolkit
 - <https://www.ncsc.gov.uk/collection/board-toolkit>
- For medium and larger charities (can be used in tandem with the Board Toolkit), 10 Steps to Cyber Security
 - <https://www.ncsc.gov.uk/news/large-uk-organisation-10-steps-stay-ahead>



What can you do?

- Updated risk assessments
- Cyber improvement plan/strategy
- Implement controls, review effectiveness, test
- Obtain cyber security insurance
- Create a 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