Security for CIS

Chris Hankin

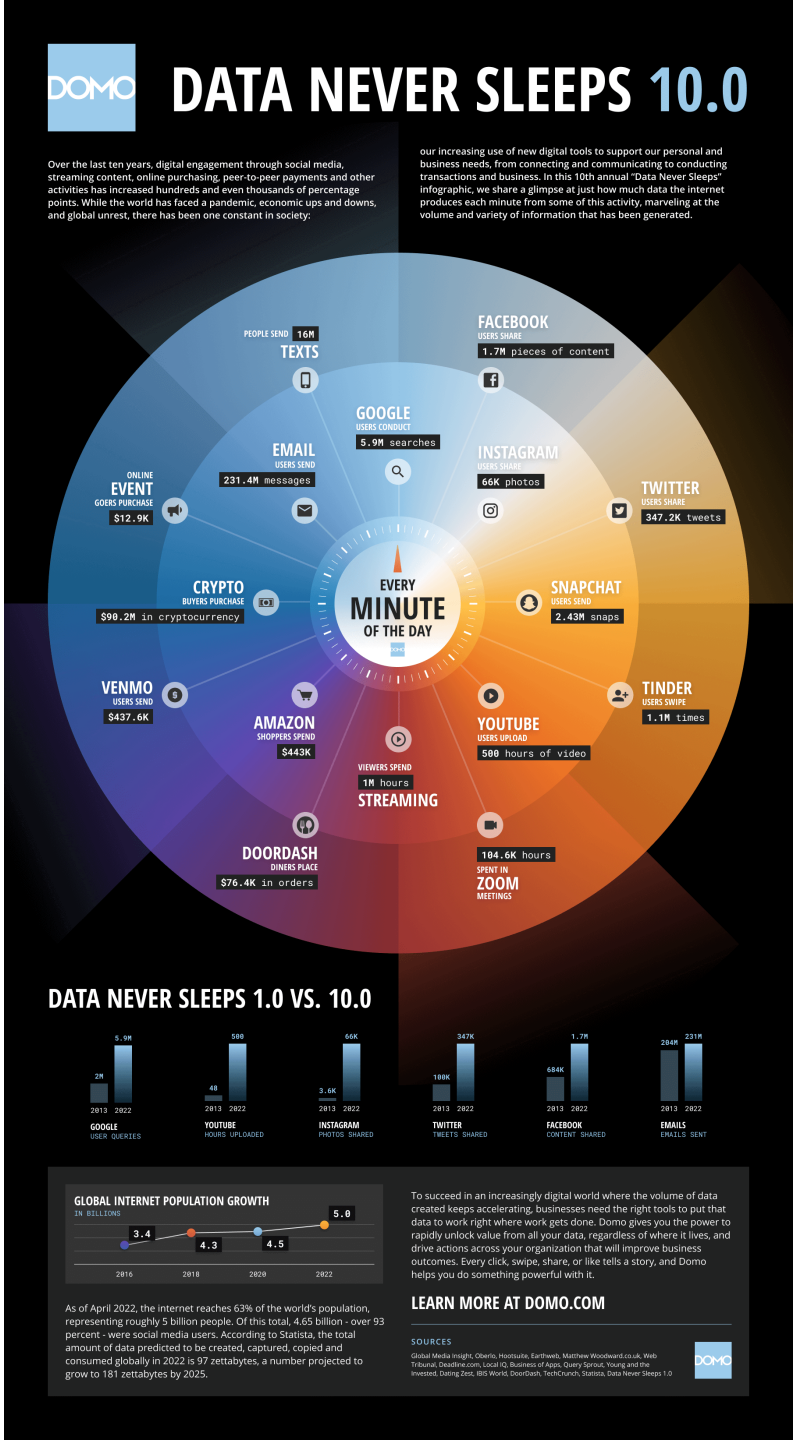

VT50 COLOUR CONTROL

50 years of Development

- Digital Equipment Corporation PDP11
- 32Kword/64Kbyte Core Memory
- Single platter disk with 5.2Mbyte capacity
- No internet

- Apple iPhone XS
- 256 Gbyte Semi-conductor memory
- WiFi, Bluetooth, Mobile network

And the volume of data that we generate keeps growing:



Cyber Security

"The protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures."

Various NCSC documents, 2016 onwards

Cyber Security

"The protection of internet connected systems, the data on them, and the services that they provide, from unauthorized access, harm or misuse"

NCSC, Third Annual Report, 2019

Alternatively, the 800+ pages of www.cybok.org

The CIA Triad

- Confidentiality: protecting information from unauthorized access.
- Integrity: maintaining and assuring the accuracy and completeness of data throughout its lifetime.
- Availability: ensuring that information is available when it is needed.

Or, The Parkerian Hexad

- CIA plus
- Authenticity: relating to veracity of the provenance of the information.
- Control: concerning the possession of the information.
- Utility: concerning the usefulness of the data (for example a breach of utility would be the loss of the key for encrypted data).

Threat Actors

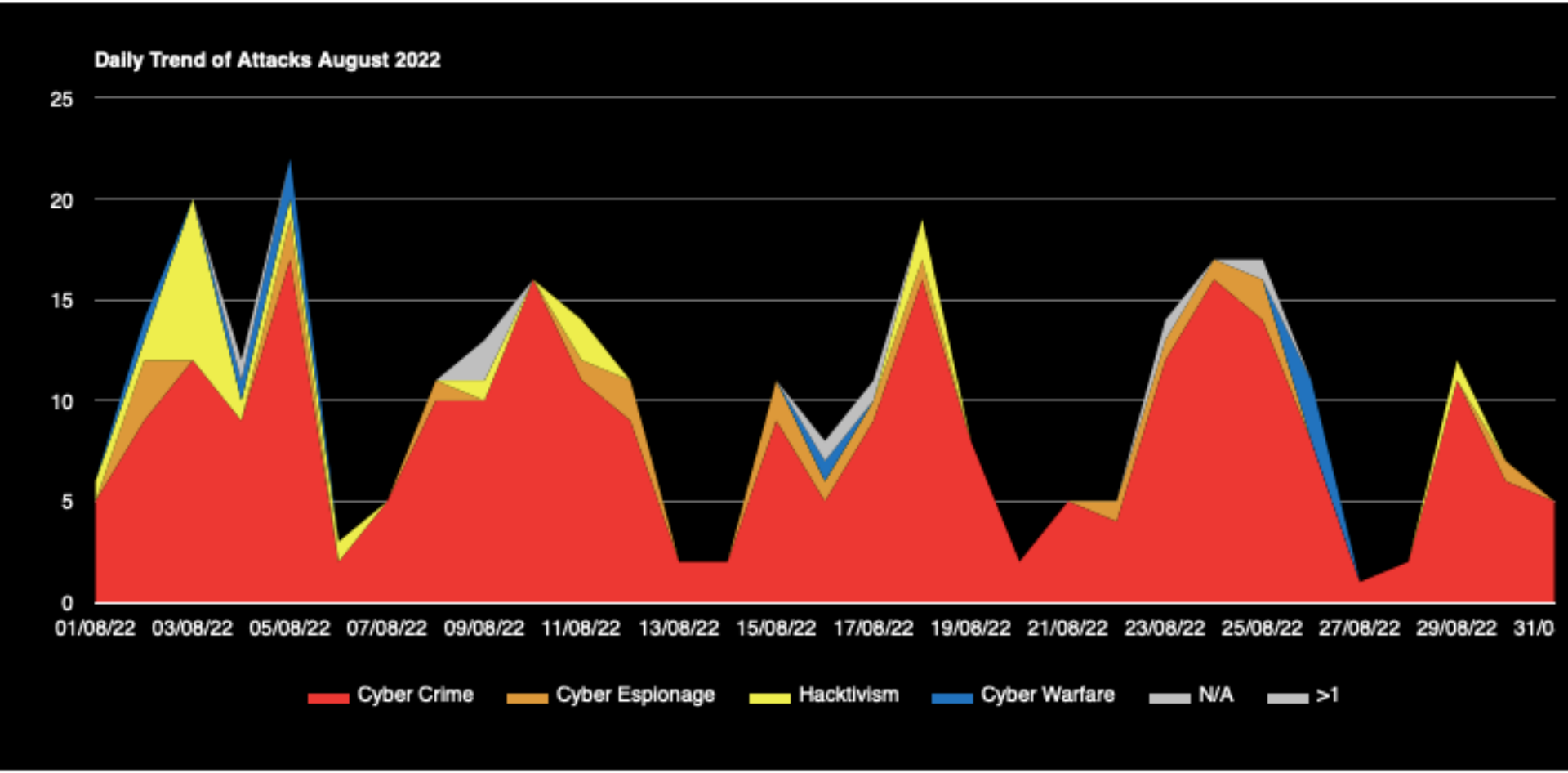
- Cyber Criminals
- State Actors
- Terrorists
- Hacktivists
- Script Kiddies

- Insiders

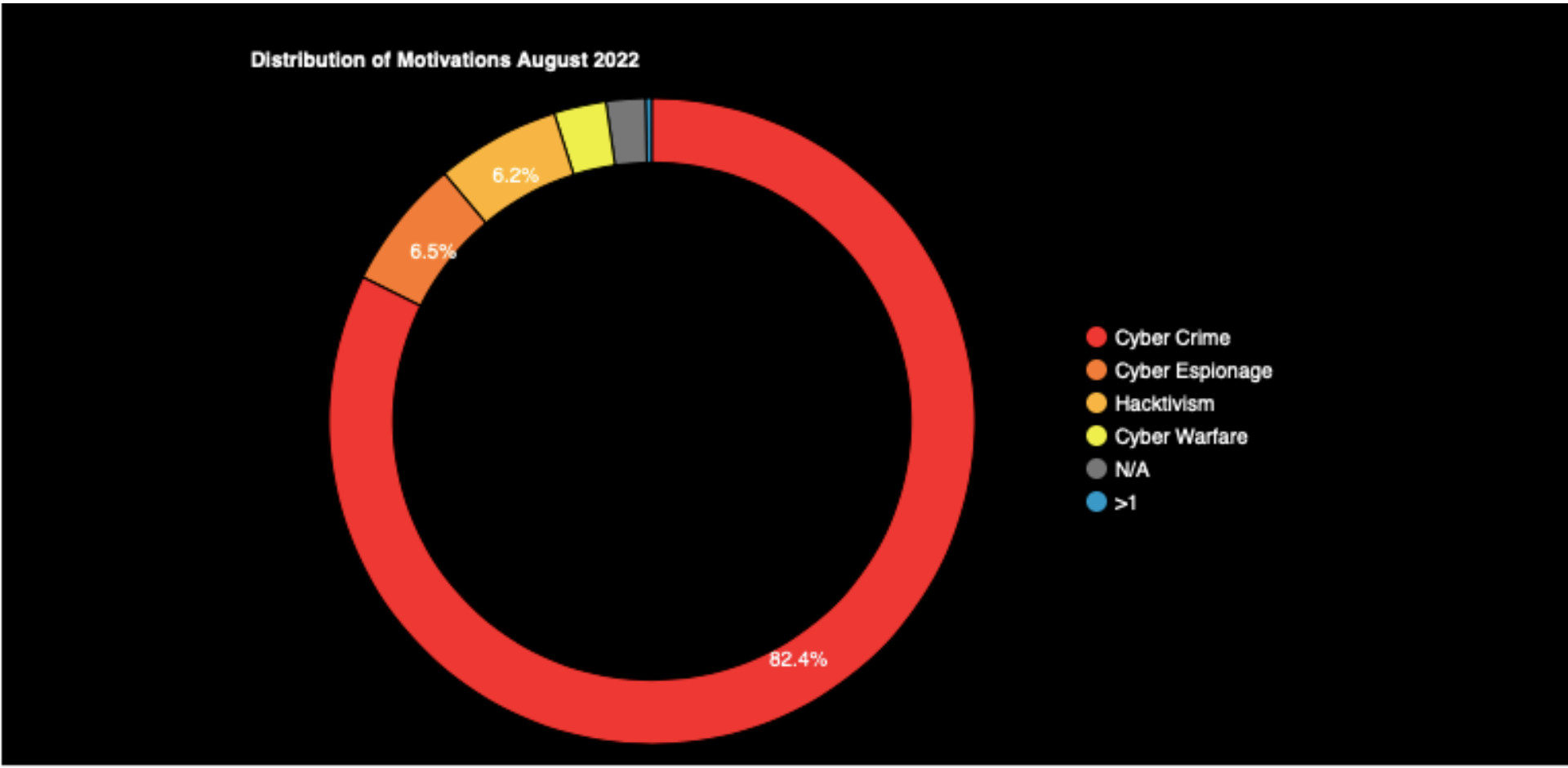
Vulnerabilities

- Expanding range of devices
- Poor cyber hygiene and compliance
- Insufficient training and skills
- Legacy and unpatched systems
- Availability of hacking resources

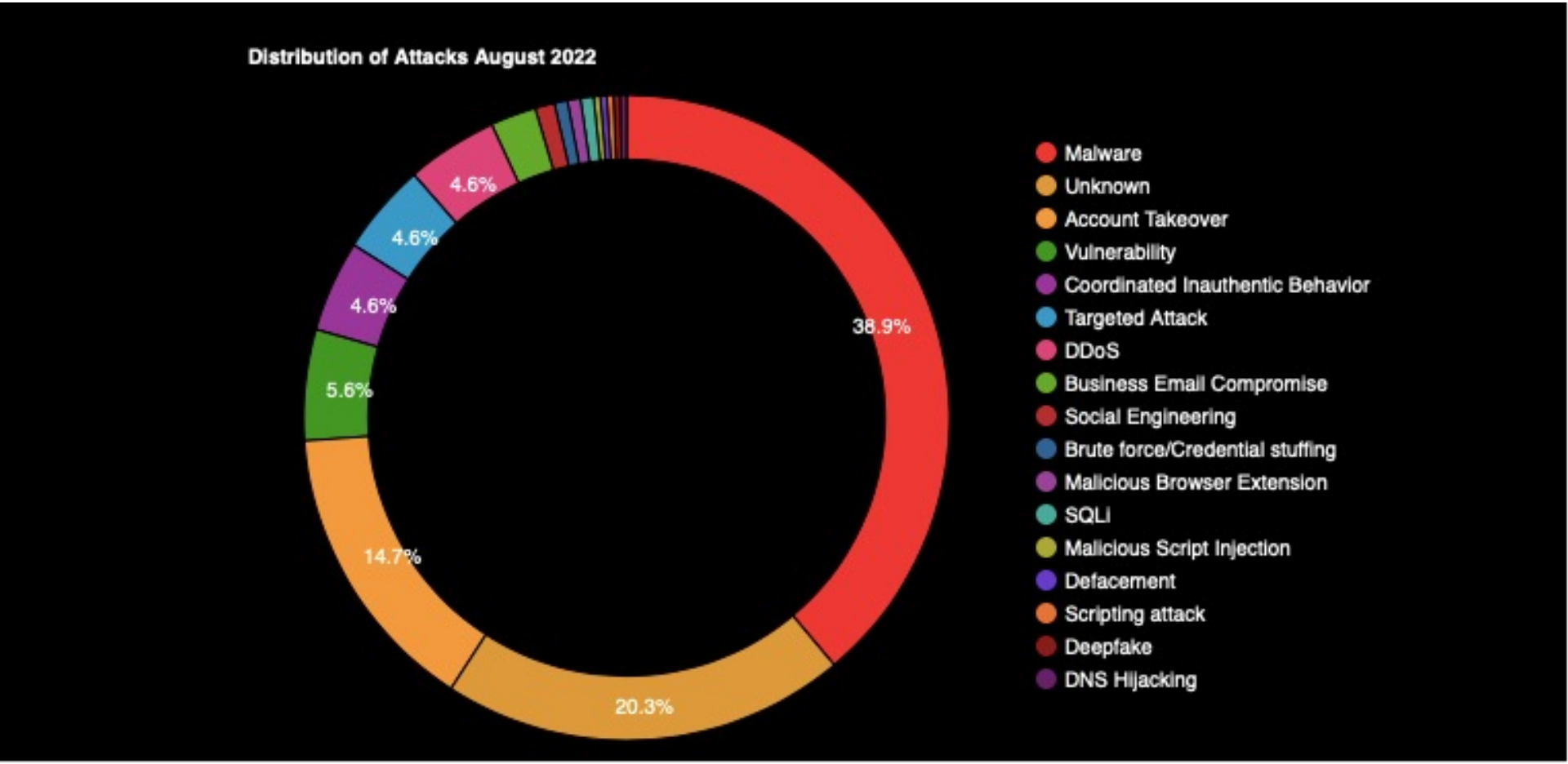
August 2022 Attacks from Hackmageddon.com (306 events)



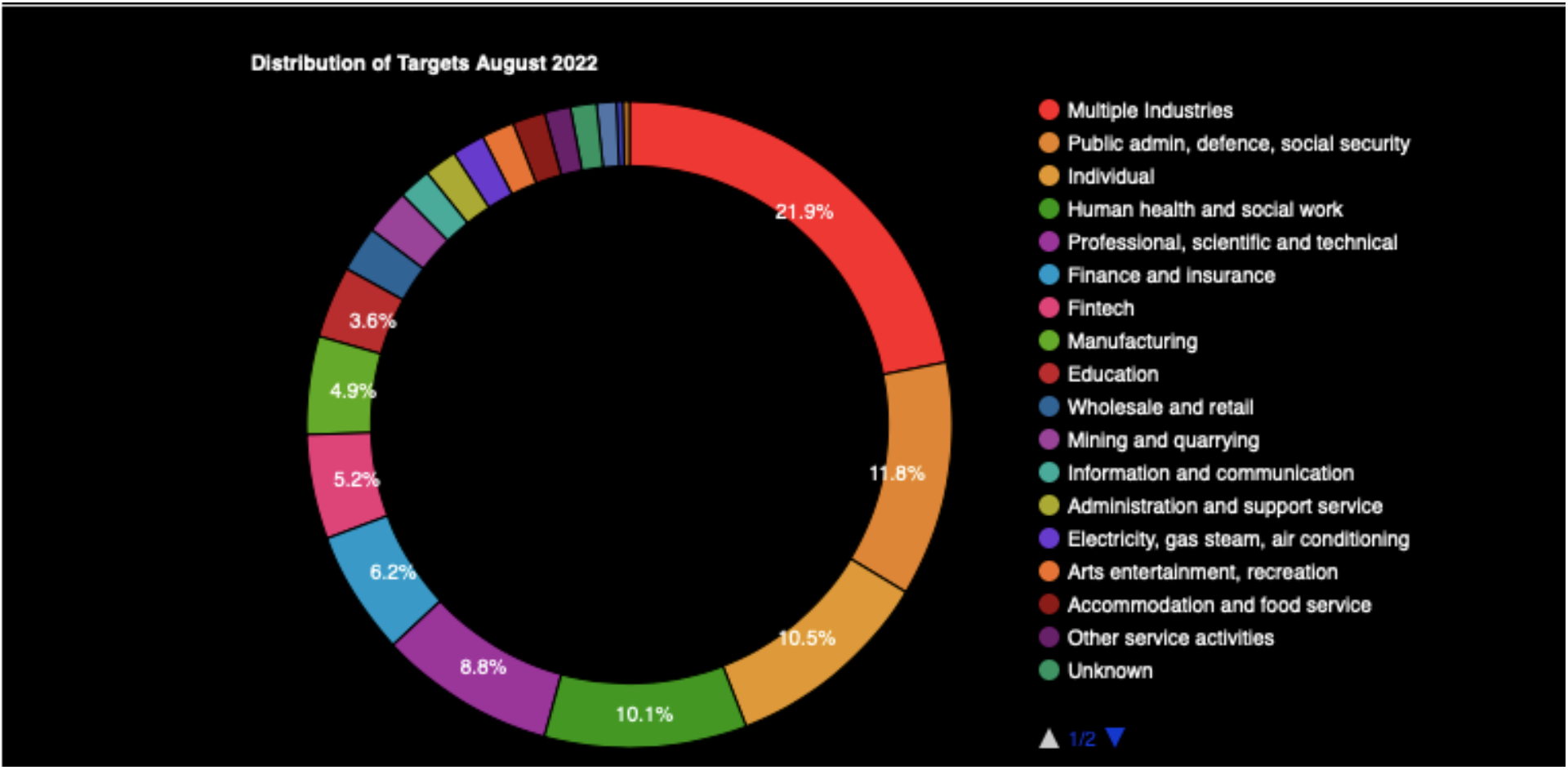
August 2022 contd.



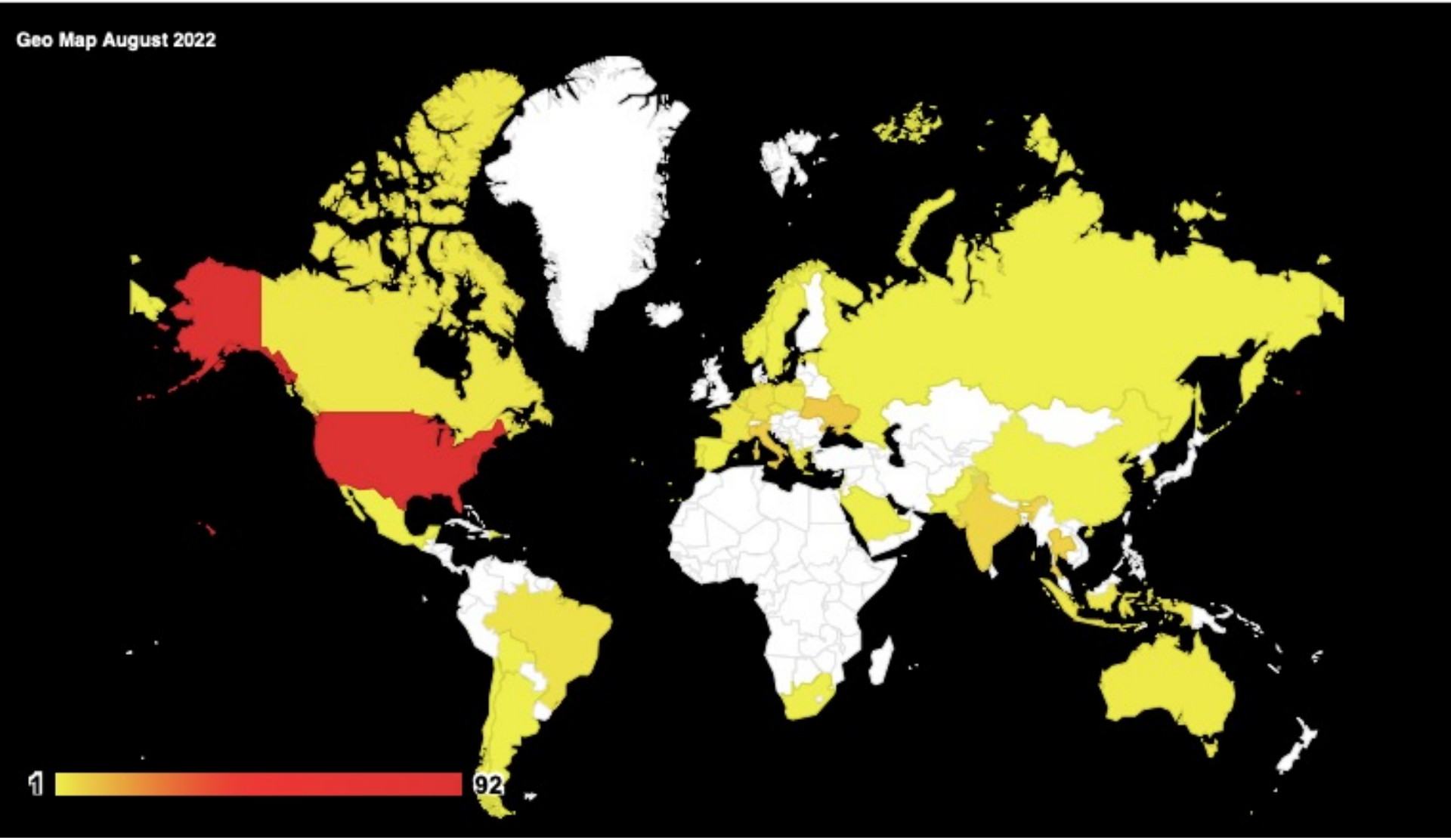
Techniques


Distribution of Attacks August 2022
38.9%
20.3%
14.7%
5.6%
4.6%
4.6%
4.6%
Malware
Unknown
Account Takeover
Vulnerability
Coordinated Inauthentic Behavior
Targeted Attack
DDoS
Business Email Compromise
Social Engineering
Brute force/Credential stuffing
Malicious Browser Extension
SQLi
Malicious Script Injection
Defacement
Scripting attack
Deepfake
DNS Hijacking

Targets


Distribution of Targets August 2022
21.9%
11.8%
10.5%
10.1%
8.8%
6.2%
5.2%
4.9%
3.6%
Multiple Industries
Public admin, defence, social security
Individual
Human health and social work
Professional, scientific and technical
Finance and insurance
Fintech
Manufacturing
Education
Wholesale and retail
Mining and quarrying
Information and communication
Administration and support service
Electricity, gas steam, air conditioning
Arts entertainment, recreation
Accommodation and food service
Other service activities
Unknown
1/2

Distribution



Details

19	17/08/2022	-	-	?	Forsyth County Medical Office	Forsyth County Medical Office discloses a cyber attack where suspicious emails were being sent out through the practices email system.	Account Takeover	Public admin and defence, social security	CC	US	Link
20	18/08/2022	17/08/2022	17/08/2022	Killnet	Government websites in Estonia	Estonia claims to have repelled "the most extensive cyber attacks since 2007", shortly after removing Soviet monuments in a region with an ethnic Russian majority.	DDoS	Public admin and defence, social security	H	EE	Link

DataBreaches.net
The Office of Inadequate Security

News Breach Laws About Donate XMR Contact Privacy Transparency Reports

GA: Hacker disrupts systems at Forsyth County medical office

Home / GA: Hacker disrupts systems at Forsyth County medical office

GA: Hacker disrupts systems at Forsyth County medical office

AUGUST 17, 2022 DISSENT

> On July 25, Forsyth County deputies responded to reports that the computer system
> office had been hacked.

REUTERS World Business Legal Markets Breakingviews Technology Investigations M

Europe

2 minute read · August 18, 2022 9:42 PM GMT+1 · Last Updated 2 months ago

Estonia says it repelled major cyber attack after removing Soviet monuments

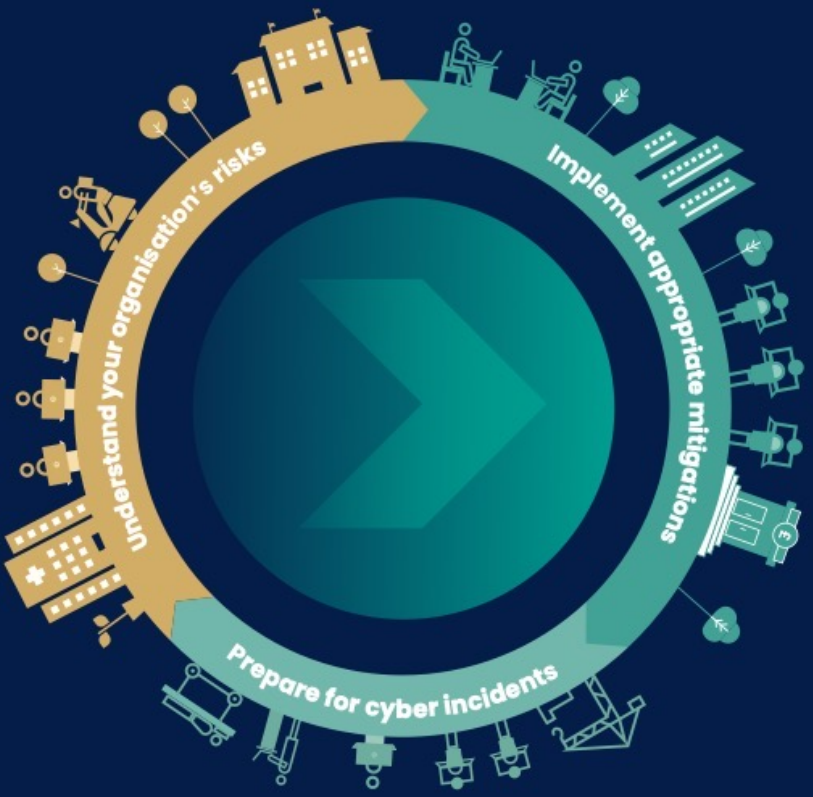
By Andrius Sytas

National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

- **Risk management**
  Take a risk-based approach to securing your data and systems.
- **Engagement and training**
  Collaboratively build security that works for people in your organisation.
- **Asset management**
  Know what data and systems you have and what business need they support.
- **Architecture and configuration**
  Design, build, maintain and manage systems securely.
- **Vulnerability management**
  Keep your systems protected throughout their lifecycle.



- **Identity and access management**
  Control who and what can access your systems and data.
- **Data security**
  Protect data where it is vulnerable.
- **Logging and monitoring**
  Design your systems to be able to detect and investigate incidents.
- **Incident management**
  Plan your response to cyber incidents in advance.
- **Supply chain security**
  Collaborate with your suppliers and partners.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

National Cyber Security Centre

What you can do to combat cyber attacks

Reducing The Impact

Most cyber attacks are composed of four stages: **Survey, Delivery, Breach and Affect.** The following **security controls,** applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Survey

User Education

Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

Delivery

Network Perimeter Defences

Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection

Can block malicious emails and prevent mailware being downloaded from websites.

Password Policy

Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Secure Configuration

Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

£600K-£1.15m

Average cost of security breach

Breach

Patch Management

Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring

Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection

Malware protection within the internet gateway can detect malicious code in an important item.

Secure Configuration

Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access

Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training

User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls

Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Affect

Controls For The Affect Stage

Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help.

10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.

81%

of large companies reporting breach

For more information go to **www.ncsc.gov.uk** **@ncsc**

National Cyber Security Centre

Ransomware
Prevention & recovery

Following this advice can reduce the likelihood of you becoming a victim of ransomware. Ransomware makes your data or computers unusable and asks you to make a payment to release it. If your computer is already infected with ransomware, we've included some useful recovery steps below. For more information, please refer to **www.ncsc.gov.uk/ransomware** .

What is ransomware?

Ransomware is malicious software that prevents you from accessing your computer (or data that is stored on your computer).

If your computer is infected with ransomware, the computer itself may become **locked**, or the data on it might be **stolen**, **deleted** or **encrypted**.

Normally you're asked to make a payment (the ransom), in order to 'unlock' your computer (or to access your data).

However, even if you pay the ransom, there is no guaranteethat you will get access to your computer, or your files. This is one of the reasons why it's important to **always have a recent backup** of your most important files and data.

Don't be blackmailed - keep a backup!

If you have a recent backup of your most important files, then you can't be blackmailed.

Make regular backups of your most important files (such as photos and documents), and check that you know how to restore the files from the backup. If you're unsure how to do this, you can search online.

Make sure the device containing your backup (such as an external hard drive or a USB stick) is not permanently connected to your computer.

Turn on auto-backup so that data on your smartphone is automatically copied to the cloud. This means you'll be able to recover your data quickly by signing back into your account from another device.

Protecting your data and devices

The following steps will reduce the likelihood of your devices being infected with ransomware.

Keep your operating system and apps up to date. Apply software updates promptly to help keep your device secure. This includes protection from ransomware and other types of virus. Set updates to happen automatically, so you don't forget.

Make sure your antivirus product is turned on and up to date. Windows and macOS have built in malware protection tools which are suitable for this purpose.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses.

What to do if you are infected

If your computer has been infected by ransomware (or any type of malware), you should:

Open your antivirus (AV) software, and run a full scan. Follow any instructions given. If your AV can't clean your device, you'll need to perform a 'clean re-install', which will remove all your personal files, apps and settings. If you're unsure how to do this, you can search online using another device, or ask family and friends.

Restore your backed-up data that you have kept on a separate device (such as USB stick, external hard drive) or cloud storage. Do not copy any data from the infected computer.

If you receive a phone call offering help to clean up your computer, hang up immediately (this is a common scam).

Anyone who thinks they may have been subject to a ransomware attack should contact Action Fraud (www.actionfraud.police.uk). Organisations should call 0300 123 2040. In Scotland, contact the police by dialing 101.

Should I pay the ransom?

Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. If you do pay the ransom:

- **there is no guarantee that you will get access to your data or computer**
- **your computer will still be infected**
- **you will be paying criminal groups**
- **you're more likely to be targeted in the future**

If you have paid any extortion demands you should report this to your local police force.

Wannacry

- Worm and Ransomware
- CVE-2017-0144 and CVE-2017-0145: both allowing remote attackers to execute arbitrary code exploiting a vulnerability in Windows SMBv1 servers (network file sharing).

- Ransom $300-$600 paid in bitcoin

WannaCry


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

WannaCry

Devices connected to the Internet

- 2020: 50B(???) devices
- Over half are IoT devices and that is growing by about 4B(???) per year
- 2030 estimates: 125B(???) to 500B(???)

- The majority of these devices will be deployed in cyber-physical systems
- Industrial Control Systems (ICS) are an extreme example

Critical infrastructure systems

- Water treatment/distribution
- Smart grid, energy, power
- Health
- Manufacturing, production facilities
- Transportation
- Oil, gas
- Telecommunications
- Others


STUXnet

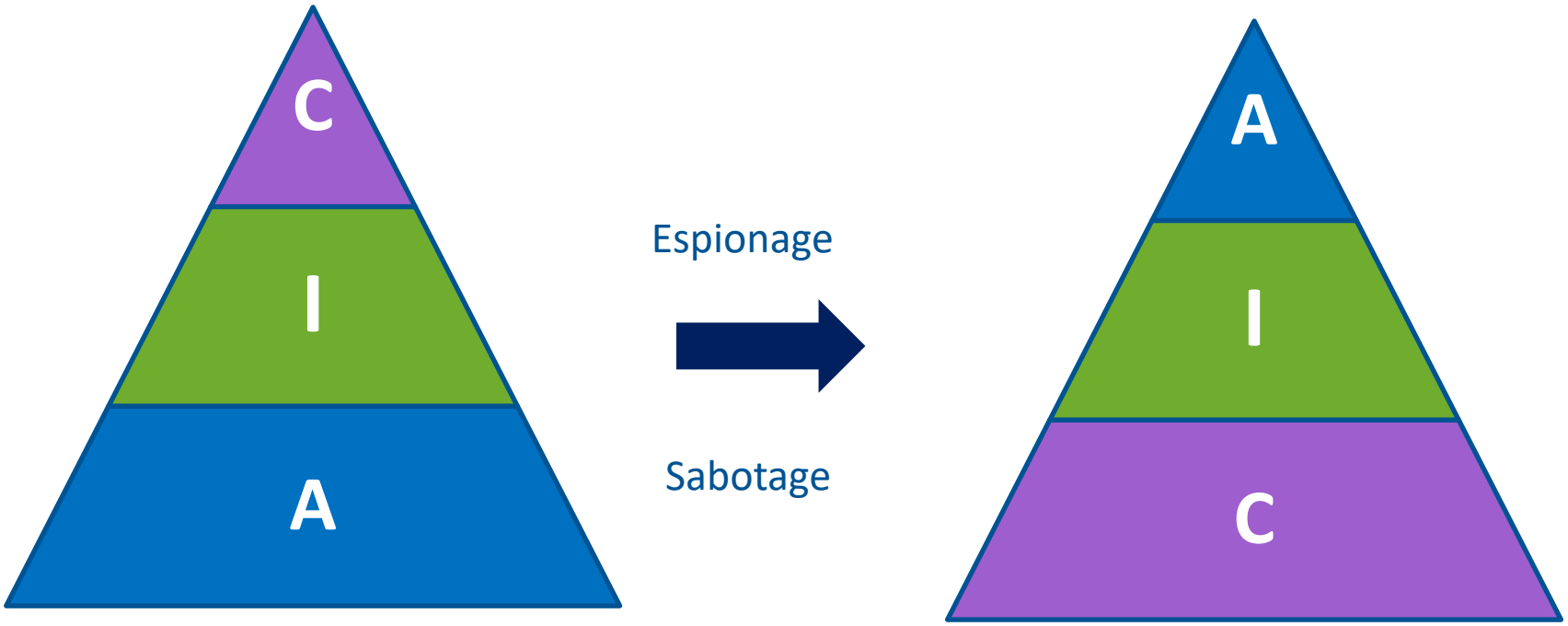
Other potential consequences

Cyber security is vital!

Some security management challenges

- Most critical systems are cyber-physical
- OT's replacement cycle differs to that of IT systems (e.g. industrial vs office-like systems)
- Operation 24/7 (maintenance planning)
- Legacy equipment and machinery
- Patching systems is not always possible (downtime, regulations, checks)
- Geographically dispersed
- Increased exposure to the Internet
- Criticality analysis, security prioritisation

A change of emphasis ...



... not forgetting: Maintainability, Reliability and Safety

What can go wrong.

- https://www.youtube.com/watch?v=fJyWngDco3g

Colonial Pipeline Attack

- Ransomware attack on 7 May 2021
- Ransom of $4.4M paid
- Attributed to DarkSide hacking group
- Pipeline restarted 12 May 2021
- $2.3M recovered

Image from BBC website

NIST Framework

CISA Alert AA21-131A - Mitigations

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

- Multi-factor authentication
- Spam filters
- User education and training
- Network filters
- Software patching
- Limit network access
- Regular scans
- Unauthorised execution prevention

CISA Alert AA21-131A - Containment

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

- Network segmentation between IT and OT
- Organise OT into logical zones
- Identify inter-dependencies between IT and OT
- Test manual controls
- Backups
- Limit user and process accounts – least privilege and separation of concerns

CISA Alert AA21-131A - Recovery

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

- Isolate infected system
- Turn off other computers and devices
- Secure back-ups

Common attacks

Buffer overflow:

```
#include <stdio.h>

int main()
{
   int x = 0;
   char buffer[6];   //allocate 6 bytes
   gets(buffer);     //grab some input
   printf("%i\n", x);
   return 0;
}
```

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

From: heartbleed.com

What leaks in practice?

We have tested some of our own services from attacker's perspective. We attacked ourselves from outside, without leaving a trace. Without using any privileged information or credentials we were able steal from ourselves the secret keys used for our X.509 certificates, user names and passwords, instant messages, emails and business critical documents and communication.

How to stop the leak?

As long as the vulnerable version of OpenSSL is in use it can be abused. Fixed OpenSSL has been released and now it has to be deployed. Operating system vendors and distribution, appliance vendors, independent software vendors have to adopt the fix and notify their users. Service providers and users have to install the fix as it becomes available for the operating systems, networked appliances and software they use.

Common attacks

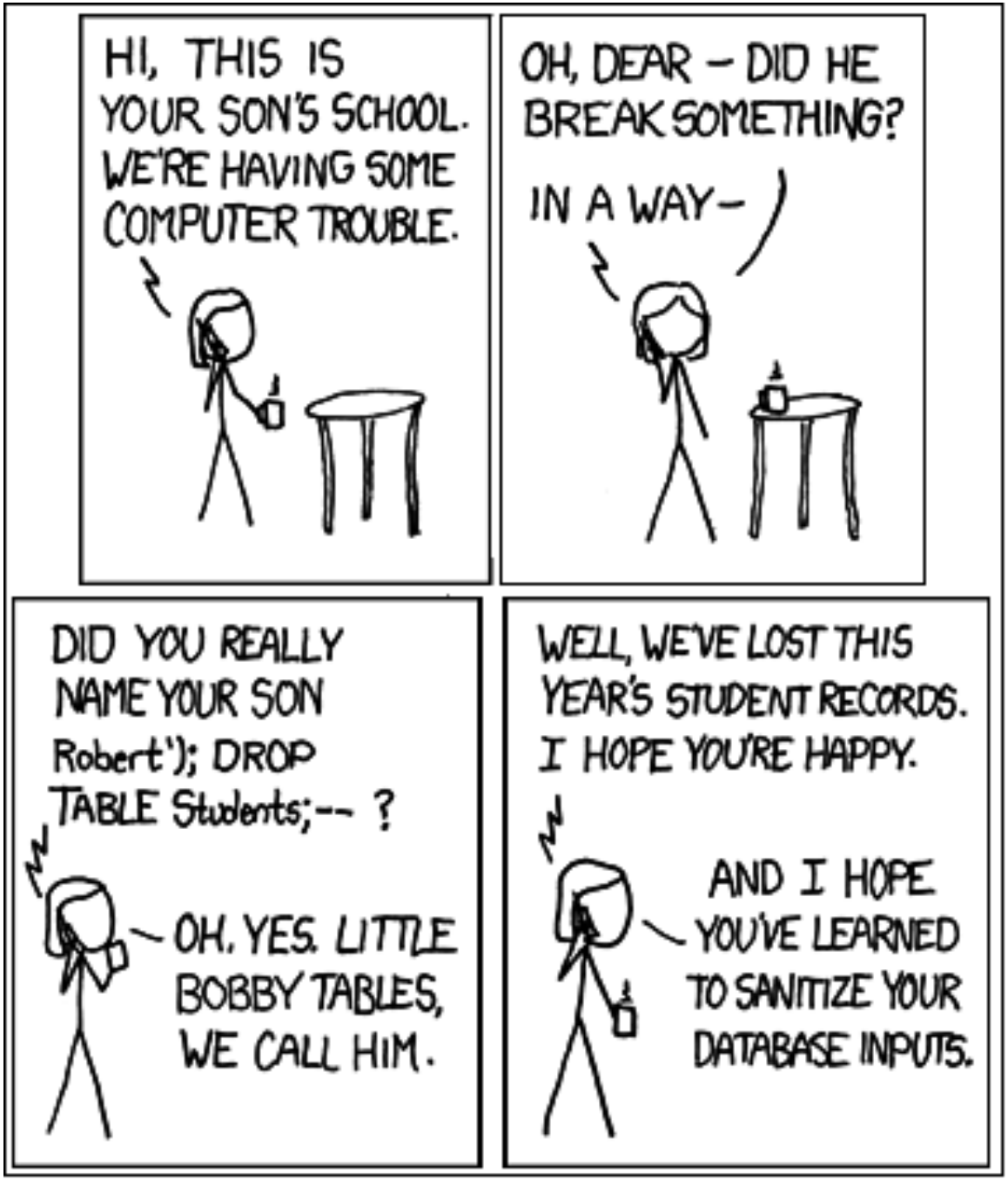
- Injection attacks (data as code):

```
UPDATE user SET password = sha1('$pwd')
WHERE username = '$usr' AND password = sha1('$old_pwd')
```

```
$pwd set to mypass
```

```
$usr set to myuser' OR 1=1 - -
```

```
UPDATE user SET password = sha1('mypass')
WHERE username = 'myuser' OR 1==1 - - ' AND password =
      sha1('$old_pwd')
```



From danielmiessler.com

UK Cyber Essentials Scheme

- Use a firewall to secure your internet connection
- Choose the most secure settings for your devices and software
- Control who has access to your data and services
- Protect yourself from viruses and other malware (anti-virus, whitelisting, sandboxes)
- Keep devices and software up to date
- cyberessentials.ncsc.gov.uk