Cyber Security Governance - Updates From The Front Line

14 July 2022

About IT Governance

The cyber risk and privacy management solutions provider

20 years of experience, 200 employees

IT governance, risk and compliance solutions

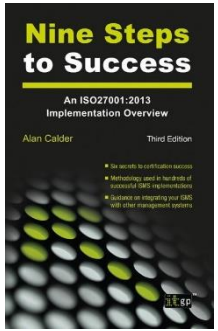
More than 12,000 clients across 6 continents

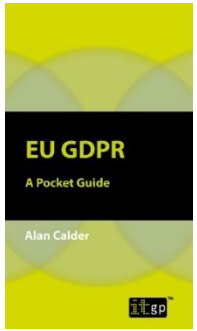
More than 1,000 penetration tests delivered

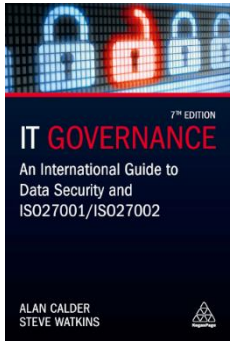
Introduction: Alan Calder

Founder and executive chairman of IT Governance

- Founder and executive chairman of IT Governance, the single source for everything to do with IT governance, cyber risk management and IT compliance.
- Author of *IT Governance: An International Guide to Data Security and ISO27001/ISO27002* (Open University textbook).







Content

01 Latest insights to protecting your business from Ransomware attacks and examples of recent attacks that have been averted.

02 Emerging Cybersecurity threats and trends.

03 Practical steps organisations should take to build cyber defence in depth

04 Q&A

Protect • Comply • Thrive

Cyber threat landscape

(World Economic Forum, 2022)

"Looking ahead to 2022-2023, cybersecurity must be seen as a strategic business issue that impacts decision-making"

Ransomware will attack a device every 2 seconds by 2031 – up from every 11 seconds in 2021 (Cybersecurity Ventures)

Cyber crime damages increasing by 15% pa to $10.5 trillion by 2025, up from $3 trillion in 2015 (Cybersecurity Ventures/MasterCard)

The SEC's proposed rules would require disclosure of two broad categories of information: cyber security incidents and cyber security risk management, strategy and governance.

Cyber security workforce gap of £2.72 million people ((ISC)^2 Research)

Threat landscape

- Increasingly sophisticated cyber criminals/serious organised crime.
- Nation-state activity and cyber warfare.
- Digitisation, migration to Cloud.

Attack surface

- Weaknesses and vulnerabilities in technology, people, process.
- Supply chain & MSP vulnerabilities – one-to-many attacks.
- Inadequate governance, risk management and compliance.

Compliance landscape – UK, EU and USA

- Data protection and privacy (e.g. GDPR).
- Cyber security (NIS, NIS 2).
- Incident reporting (EU, CISA, SEC).

Supply side

- Global shortage of cyber security and privacy professionals.
- Fragmented market.
- Multiple small, 'single solution' businesses.
- Cyber insurance increasingly expensive.

Cyber defence – warnings for a period of increased cyber risk

“From the start of the conflict in Ukraine, we have been asking organisations to strengthen their cyber-defences to help keep the UK secure, and many have done so. But it’s now clear that we’re in this for the long haul and it’s vital that organisations support their staff through this demanding period of heightened cyber threat.”

NCSC director for national resilience and strategy, Paul Maddinson.

Ransomware – the biggest online threat to UK organisations

NCSC's chief executive, Lindy Cameron, said

- “Ransomware remains the biggest online threat to the UK and we do not encourage or condone paying ransom demands to criminal organisations.
- "Unfortunately we have seen a recent rise in payments to ransomware criminals and the legal sector has a vital role to play in helping reverse that trend.
- "Cyber security is a collective effort and we urge the legal sector to work with us as we continue our efforts to fight ransomware and keep the UK safe online.“
- "We expect ransomware will continue to be an attractive route for criminals as long as organisations remain vulnerable and continue to pay."

Source: Businesses urged not to give in to ransomware cyber criminals as authorities see increase in payouts | Science & Tech News | Sky News

Reduction in cyber insurance and what it means for organisations

- The US Government Accountability Office (GAO) warned that private insurance companies are increasingly backing out of covering damages from major cyber attacks, leaving American businesses facing “catastrophic financial loss” unless another insurance model can be found.

- “Cyber insurance can help offset costs of some common cyber risks, like data breaches or ransomware. Cyber risks are growing, and cyber attacks targeting critical infrastructure, like utilities or financial services, could affect entire systems and result in catastrophic financial loss,” says the GAO report.

- The US Department of the Treasury said that insurers have also been mitigating their exposure by lowering the maximum amount that a policy will pay out in the case of a cyber attack and increasing premiums to protect themselves from losses.

The anatomy of a cyber attack

8 Stages

The cost of human error

IBM's Cost of a Data Breach Report 2021 found:

The **two most expensive forms of data breach** were the result of **'fuzzy firewall failures'**.

According to its study, BEC (business email compromise) **scams cost organisations $5.01** (about £3.75) per record stolen, and **phishing scams cost $4.61** (£3.45).

Data breaches involving **human error often take longer to identify and contain**, which means the damage can escalate.

Breaches that result from BEC and phishing were among those that take the longest to resolve. BEC scams take on average **238 days to identify and 79 days to resolve, and phishing takes 213 days to identify and 80 days to resolve.**

3 types of ransomware

What are they

Scareware

Scareware is typically little more than malicious advertising. The user might see a pop-up advising that malware has been detected and instructing them to visit a website, download a tool or make a payment to have the malware removed. This can be served on a website or from a malware infection on your device.

Screen lockers

Screen lockers, meanwhile, look a lot like encrypting ransomware. They freeze your device and often present a message stating that the user must pay a ransom or that the user is under investigation by the FBI or some other authority. This is obviously a more significant threat than scareware, but in most cases your data is safe – the malware is simply preventing you from accessing the device and is trying to scare you into making the payment.

Encrypting ransomware

Encrypting ransomware poses a much greater threat than the other types because it is not possible to recover your files without either a great deal of luck (if the ransomware is old enough that there is a known solution) or by paying the ransom – and there is no guarantee that the criminals will hold up their side of the deal.

Ransomware

Exploiting issues that are well known

Encryption of files by exploiting:

- Known vulnerabilities
- Zero days
- Weak/guessable passwords
- Insecure remote access controls
- Poorly configured wireless attacks
- USB key drops

How ransomware is delivered

There are two primary ways ransomware gains access to a computer or network:

- **Social engineering,** such as phishing - typically relies on human error – people clicking links in phishing emails, allowing an unknown application to execute.

- **Technical vulnerabilities in the network perimeter**.
  - More complicated attacks – will combine data from a number of sources in order to gain access. For instance, responses from a login portal (e.g. error outputs that make it clear if a specific username is correct even if the password is wrong) could be combined with information gleaned from LinkedIn (a list of employees) and previous data breaches (connecting a user with passwords they have previously used) to give criminals a set of likely user credentials to attempt.

- Ransomware can also be delivered a number of other ways – via a wider infection once it gets into a network, for instance, within an infected USB device, packaged with a more 'benign' download (such as bundled with an app or other software from a disreputable source), and so on. In many cases, the initial infection is due to human error or inadequate security controls.

Social engineering

Common methods

Vishing

- Bank impersonation
- Tech support fraud
- Fraud

Face to face

- Enumeration of sensitive information and policies or procedures

Physical access to a build

- Planting rogue devices
- Stealing of data and property
- Gaining access to internal systems

Insider threats and third parties

The people that have inherent trust

Using established trust to perform:	
	Social engineering
	Exploit vulnerabilities
	Zero days
	Weak/guessable passwords
	Insecure remote access controls

Examples of ransomware attacks

How it affects your organisation

- Two especially notable ransomware data breaches were WannaCry and Colonial Pipeline because they affected the public, not just IT systems, which made the need to resolve the situation much more urgent and increased the likelihood that the ransoms would be paid.

In 2017, the WannaCry ransomware attack crippled around a quarter of a million computers and brought the NHS to a standstill. In a lucky turn, the attackers had left a loophole that stopped the infection in its tracks after a few days, but the damage was still considerable and the attackers made off with about £100,000 in ransom payments.

In 2021, the Colonial Pipeline – which supplies nearly half of the fuel used by the east coast of the US – was knocked offline by a clearly targeted ransomware attack, leading President Biden to declare a state of emergency.

Microsoft Exchange Server

Cyber attack example

- In January 2021, suspicious activity was detected and linked to four zero-day vulnerabilities in on-prem Microsoft Exchange Servers.
- In March 2021, it was reported that the Microsoft hack affected at least 30,000 US organisations including local governments and the malware was discovered on over 2000 machines belonging to businesses in the United Kingdom.
- The UK government joined the US and others, claiming the cyberattack was the work of Chinese state-sponsored hackers.

Recognise:

- Attackers hack known vulnerabilities;
- Vulnerabilities are prolific;
- Nation-state attackers will also impact ordinary businesses;

Respond:

- Immediate action to download and install patches;
- Ongoing penetration testing to ensure that your systems are patched;

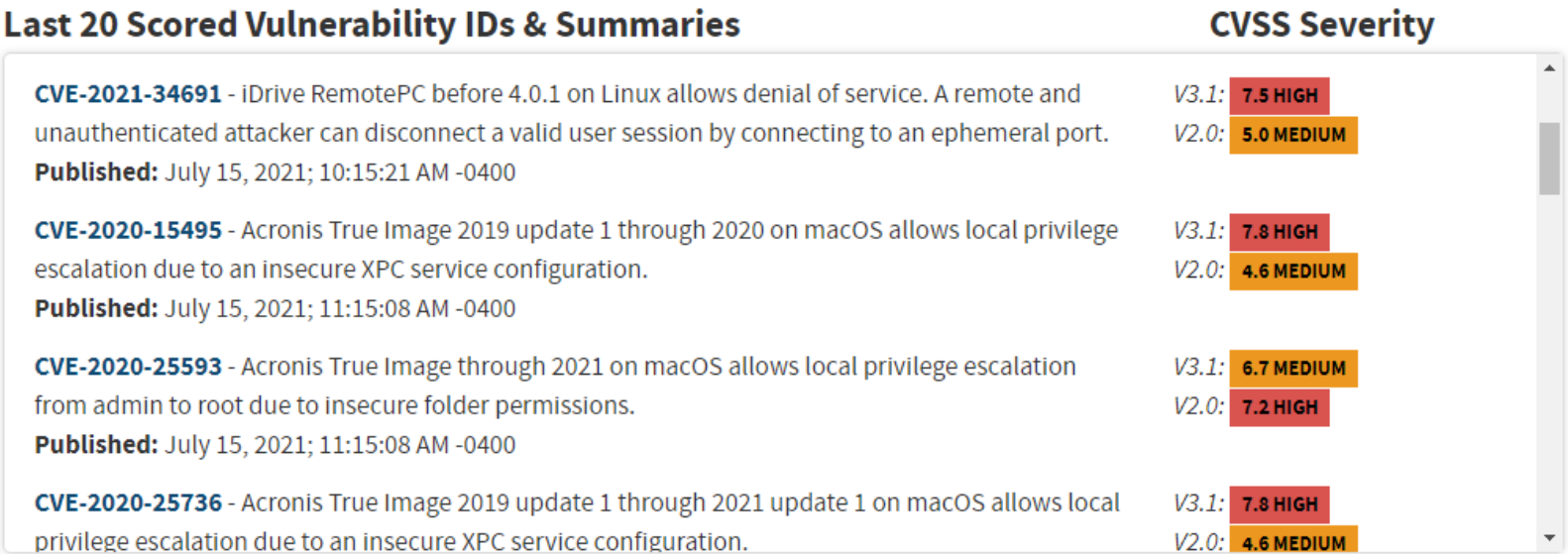
Conclusion:

- Regular penetration tests help businesses identify vulnerabilities and implement controls to reduce risk

CVE database

CVE and NVD Relationship

- Publicly available record of all known vulnerabilities – also available to attacks;
- Cyber criminals can craft attacks specifically to attack known vulnerabilities.



Emerging cybersecurity threats and trends

2022

43% of cyber attacks target small businesses

- Accenture's Ninth Annual Cost of Cybercrime Study found that 43% of data breaches occur at SMEs.

83% of SMEs aren't equipped to recover from a cyber attack

- According to an InsuranceBee survey, 83% of SMEs aren't financially prepared to recover from a cyber attack.

3.1 billion spoofed emails are sent every day

- Spam emails are a continual threat, with a Proofpoint study revealing that 3.1 billion messages are sent every day.

Scam messages have cost businesses €23 billion since 2016

- As evidence of how successful those scams are, Proofpoint adds that organisations have been scammed out of $26 billion (about €22.7 billion) since 2016. That's an average of about €3.6 billion per year.

Organisations spend €3.4 million responding to cyber attacks

- A Ponemon Institute study found that organisations spend $3.86 million (about €3.4 million) recovering from cyber attacks.

Strong incident response can save organisations €1.1 million

- A key figure in the Ponemon Institute report relates to threat detection: organisations that can identify and contain a data breach within 200 days reduce their costs by about €1.1 million.

Remote workers increase the cost of a data breach

- Another factor that impacts the cost of a data breach is whether employees work from home. The Ponemon Institute report found that organisations that have adopted remote working spend an additional $1.07 million (about €930,000) responding to data breaches.

Emerging cybersecurity threats and trends

2022 continued

47% of organisations will let employees work remotely after the pandemic	• According to a Gartner survey, 47% of organisations will give employees the option of working remotely on a permanent basis. Meanwhile, 82% said they will let staff work from home at least one day a week.
Phishing was used in 36% of cyber attacks	• Verizon's 2021 Data Breach Investigations Report found that 36% of all breaches involved phishing.
Criminals received €4.5 million in Bitcoin through ransomware extortion	• According to a FinCEN report, ransomware extortions have resulted in at least $5.2 billion (about €4.5 billion) in Bitcoin transactions.
82% of organisations have increased their cyber security budget.	• Accenture's State of Cybersecurity Resilience 2021 report found that 82% of organisations said they increased their cyber security budget in the past year.
Only 9% of organisations have purchased cyber insurance	• Many believe that cyber insurance will become essential in 2022, as the financial risks related to data protection become increasingly burdensome. However, according to InsuranceBee, only 9% of organisations currently have cyber liability insurance.
The cyber security skills gap has decreased by 400,000	• Cybersecurity Workforce Estimate found that the skills gap shrank in 2021. The influx of cyber security professionals means there are now 2.72 million unfilled roles, compared to 3.12 in the previous year.

Practical steps organisations should take to build cyber defence in depth

IT governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

How to build cyber defence in depth strategy

Organisations should take a risk-based approach to preventing cyber attacks.

1st line	**LARGELY DETECTIVE:** Continual vulnerability scanning, authentication policy and phishing staff awareness training
2nd line	**LARGELY PREVENTIVE:** Penetration testing, incident reporting, Cyber Essentials, security-trained IT support, and cyber security and GDPR staff awareness training
3rd line	**LARGELY PREVENTIVE, BUT MORE MATURE:** Embedded, risk-based security controls (e.g. ISO 27001 certification)
4th line	**CORRECTIVE:** Supply chain security management, business continuity management, IT disaster recovery
5th line	**RECOVERY:** Cyber security insurance

Practical steps to build cyber defence in depth

Take a risk-based approach to preventing cyber attacks

Step 1: Detect

Vulnerability scanning

Quickly identify exploitable vulnerabilities and misconfigurations in your websites, applications, and infrastructure.

Find out more

Step 2: Protect

Phishing awareness

Training your staff to recognise phishing emails and take appropriate action is one of the most important things you can do to keep your organisation secure. Educate employees so they can enforce best practices and reduce your risk of a successful attack or breach.

Find out more

Practical steps to build cyber defence in depth

Take a risk-based approach to preventing cyber attacks

Step 3: Manage

Cyber Security Incident Response

An experienced incident response specialist will work with you to ensure that your organisation has appropriate policies, processes, procedures and systems in place to respond to a cyber incident.

Find out more

Step 4: Respond

Data Breach Reporting

We will help you respond to an incident or a data breach quickly and in line with the GDPR's 72-hour reporting requirement so that you can resume your normal business operations with minimal disruption and hassle.

Find out more

Step 5: Recover

Cyber Security as a Service

Let our cyber security consultants, legal experts and incident responders become an extension of your in-house IT department – we are your comprehensive cyber security team that works 24/7 to make sure you are, and remain, cyber secure.

Find out more

Cyber Safeguard

Safeguard your organisation from cyber threats and gain peace of mind with up to £500,000 of cyber insurance

- Cyber Safeguard provides all the essential support, training, testing and insurance cover you need for a cyber secure business.

Access cyber insurance cover from day one.
Quickly roll out staff awareness training and track staff participation, both in the office and remotely.
Ensure staff are appropriately trained to spot phishing emails, avoid email misuse and adhere to data privacy and information security best practices.
Perform unlimited scans to check for vulnerabilities and use your ‘Scanned by IT Governance’ badge to demonstrate to clients that you take security seriously.
Access emergency cyber incident and breach support whenever and however you need it.
Gain peace of mind with advice from legal and cyber security experts.

Find out more

Get in touch

How you can find us

United Kingdom

Visit our website
www.itgovernance.co.uk

Email us
servicecentre@itgovernance.co.uk

Call us
+44 (0)333 800 7000

Join us on LinkedIn
/company/it-governance

Follow us on Twitter
/ITGovernanceLtd

Like us on Facebook
/ITGovernance

Europe

Visit our website
www.itgovernance.eu

Email us
servicecentre@itgovernance.eu

Call us
+353 (0) 1 695 0411

Join us on LinkedIn
/company/it-governance-europe-ltd

Follow us on Twitter
/itgovernanceeu

Like us on Facebook
/ITGovernanceEU

United States

Visit our website
www.itgovernanceusa.com

Email us
servicecenter@itgovernanceusa.com

Call us
+1 877 317 3454

Join us on LinkedIn
/company/it-governance-usa-inc

Follow us on Twitter
/ITGovernanceUSA

Like us on Facebook
/ITG_USA

Questions

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive