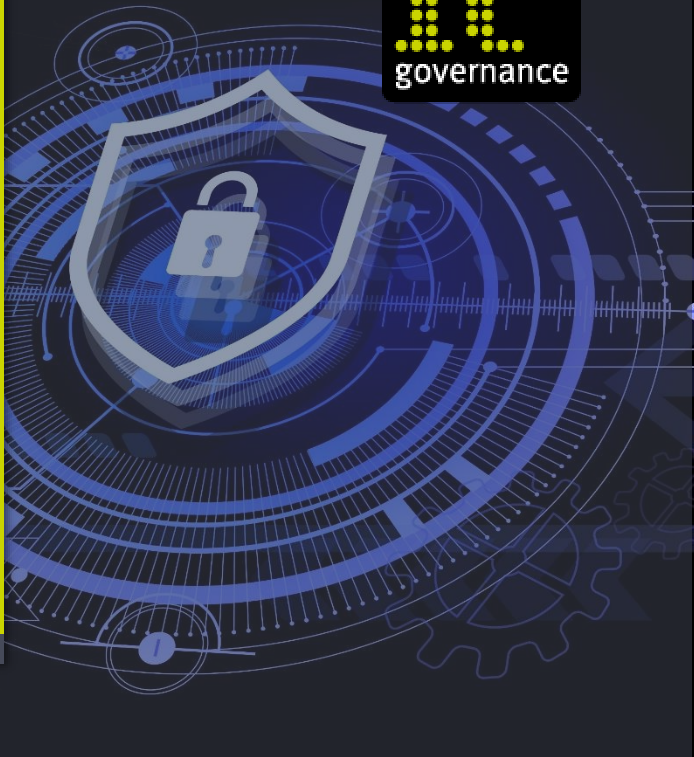
Review & strengthen cyber security governance in 2021

Protecting data and communications in a digitally-connected market

Alan Calder, Founder and CEO, IT Governance

25 March 2021



01 **Introduction**

02 **The threat landscape**

03 **Major cyber attacks and data breaches**

04 **Security and Privacy: Two Sides of the Same Coin**

05 **The board and senior managers: Managing cyber exposure**

06 **Contact details**

07

1. Understand the risk
2. Take action

it governance™

Protect • Comply • Thrive

Introduction

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

About us

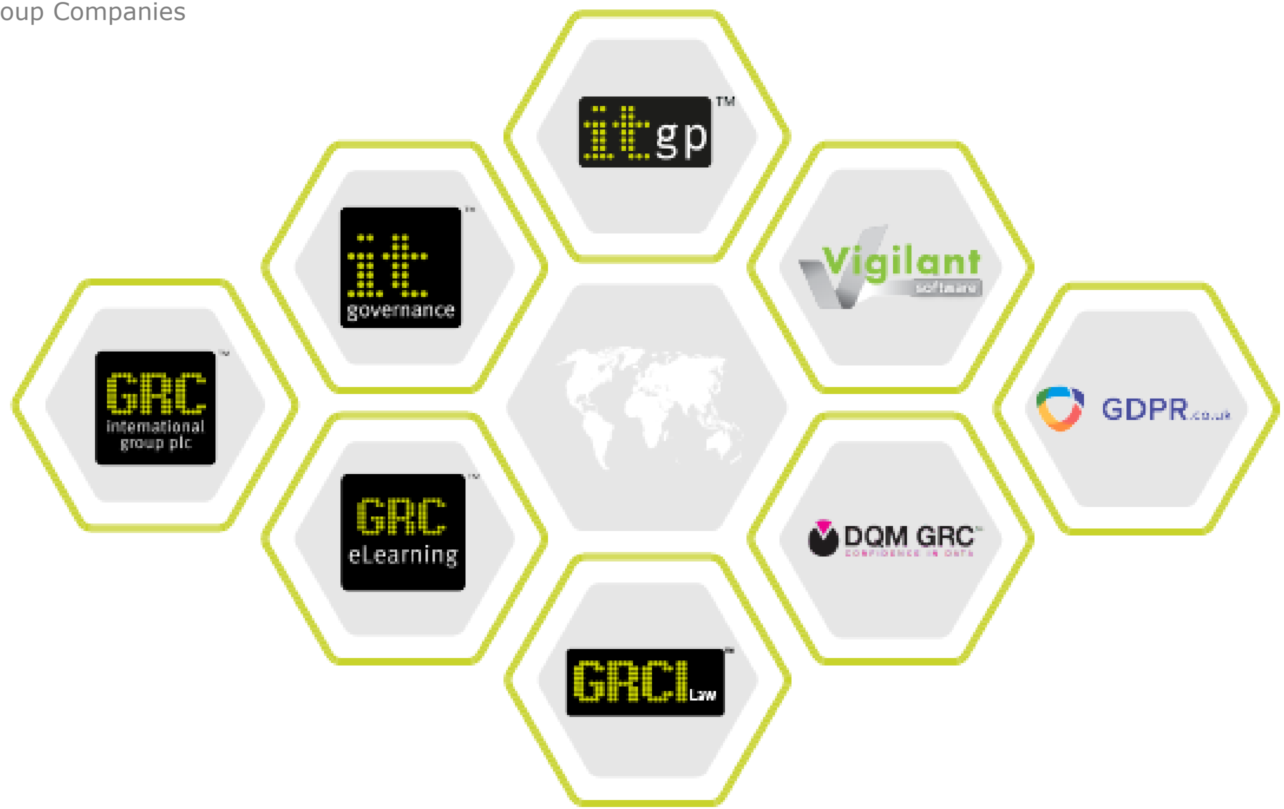
IT Governance is a leading global provider of cyber risk and data privacy management solutions.

- We deliver projects all over the world to clients across the spectrum of cyber security and resilience, data privacy, incident response and business continuity.
- Our unique and unrivalled blend of products and services include bespoke and fixed-price consultancy, training, toolkits, software, staff awareness e-learning and penetration testing.
- We pride ourselves on our ability to serve an international customer base and deliver a broad range of integrated, high-quality solutions globally, while meeting the real- world needs of today’s organisations, directors and practitioners.
- IT Governance is a subsidiary of GRC International Group plc, focused on delivering IT governance, risk management and compliance solutions.

Our Protect ● Comply ● Thrive approach is aimed at helping your organisation achieve resilience in the face of constant change.

Group overview

GRC International Group Companies



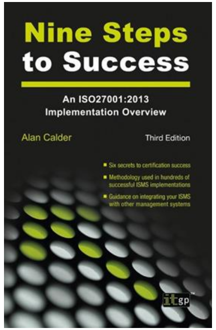
Introduction

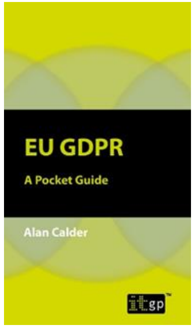
Alan Calder, Founder and executive chairman of IT Governance

- IT Governance is the leading global provider of IT governance, risk management and compliance solutions.
- Author of *IT Governance – An International Guide to Data Security and ISO27001/ISO27002* and many other books on cyber security, compliance and governance.

IT Governance has a team of 35 experienced consultants, covering the entire range of GRC disciplines. We typically recruit additional consultants to meet specific project requirements and we are currently increasing the depth of our ICS/OT resource to meet the requirements of our growing CNI consultancy practice.

IT
GOVERNANCE
6th Edition
AN INTERNATIONAL GUIDE TO DATA SECURITY AND ISO27001/ISO27002
ALAN CALDER & STEVE WATKINS


Nine Steps to Success
An ISO27001:2013 Implementation Overview
Alan Calder
Third Edition
Six secrets to certification success
Methodology used in hundreds of successful ISMS implementations
Guidance on integrating your ISMS with other management systems
itgp

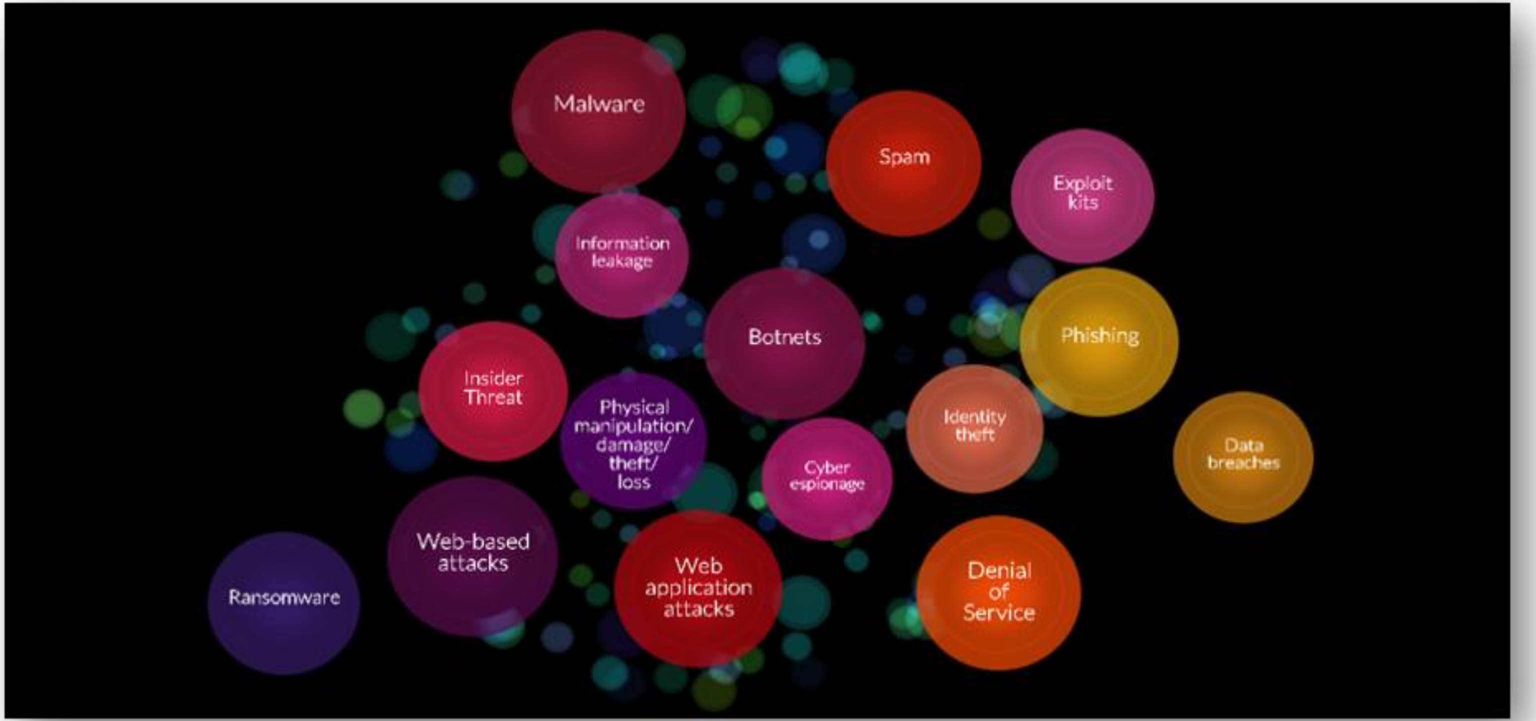


The threat landscape

Our Expertise,
Your Peace of Mind

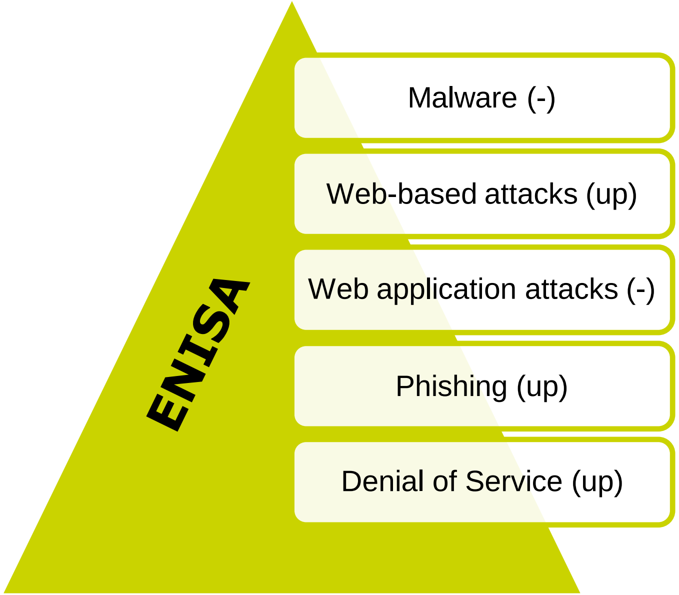
Threat landscape

The European Union Agency for Cybersecurity (ENISA) Threat Landscape Report 2020



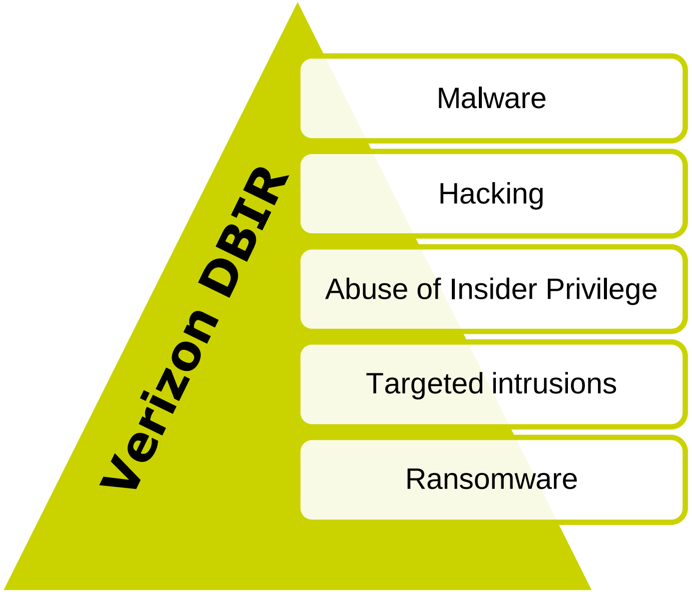
Source: ENISA Threat Landscape 2020 - List of top 15 threats — ENISA (europa.eu)

TOP 5 ATTACKS: 2020



ENISA

- Malware (-)
- Web-based attacks (up)
- Web application attacks (-)
- Phishing (up)
- Denial of Service (up)



Verizon DBIR

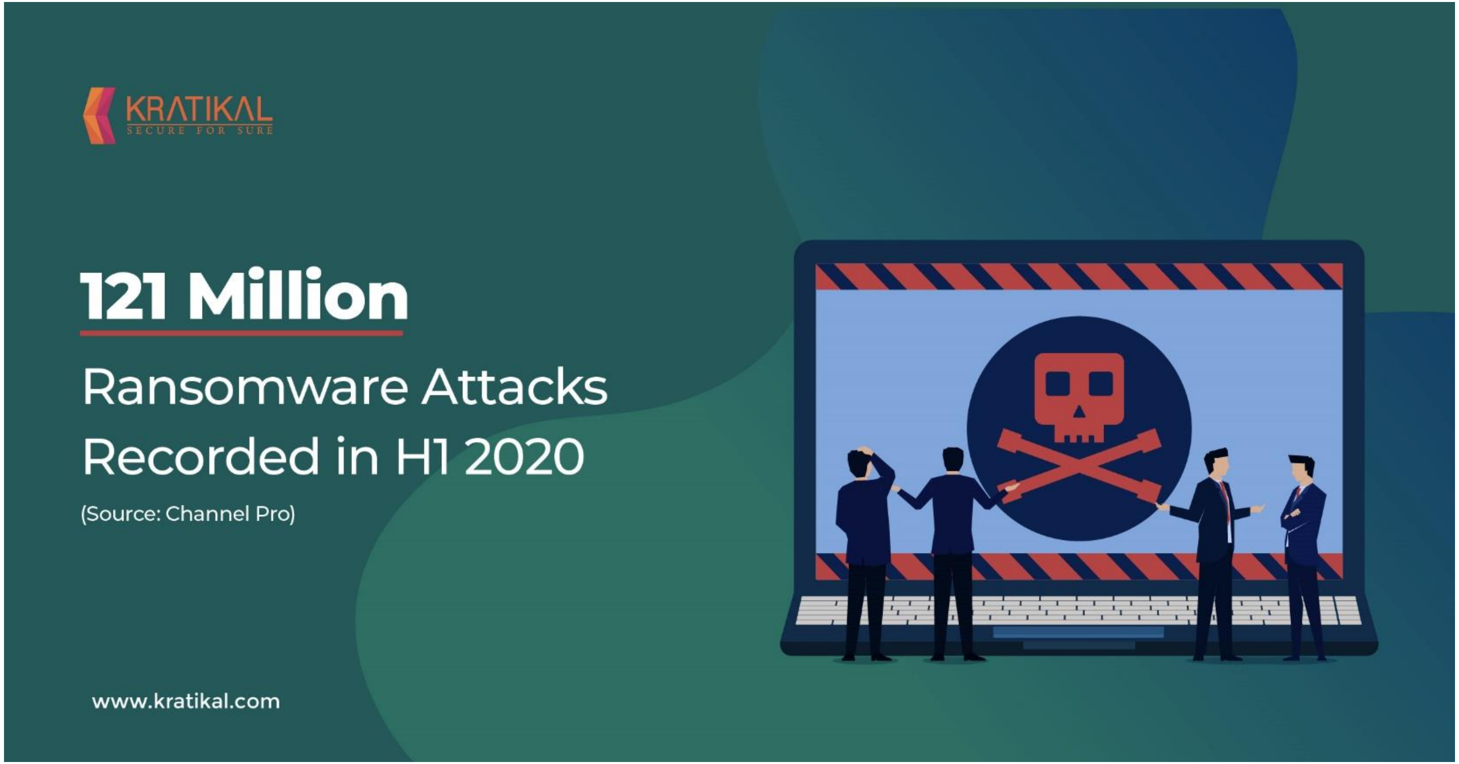
- Malware
- Hacking
- Abuse of Insider Privilege
- Targeted intrusions
- Ransomware

Multiple vulnerabilities expose organisations.

Bad actors exploit uncertainty to attack weaknesses.

- Phishing / BEC attacks
- Weak passwords / password reuse
- Malicious software / Ransomware
- Patch management
- Cloud vulnerabilities
- Insider threats (Malicious and accidental)
- Insecure configurations

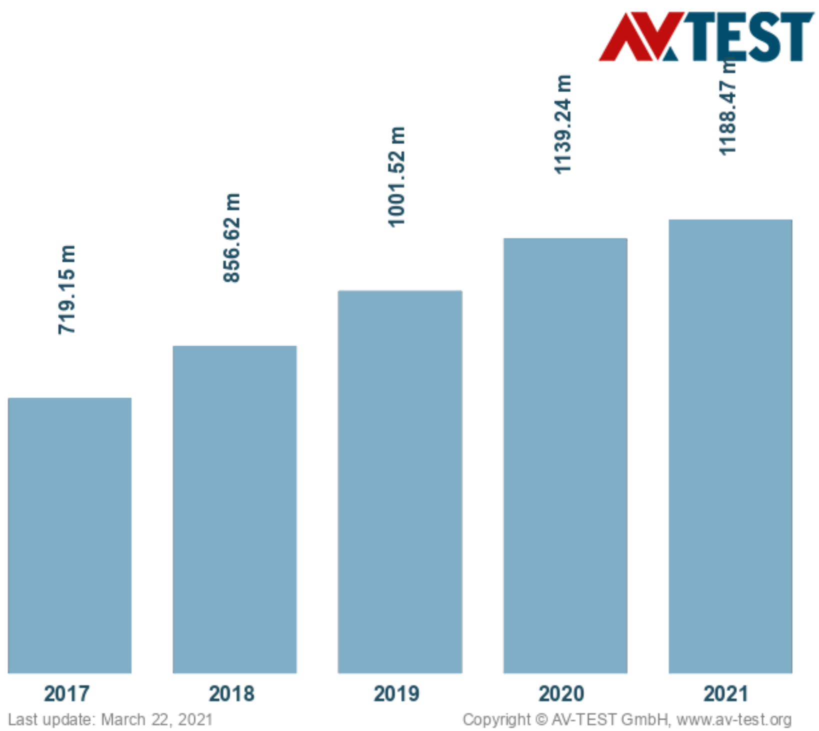
Ransomware


KRATIKAL
SECURE FOR SURE
121 Million
Ransomware Attacks
Recorded in H1 2020
(Source: Channel Pro)
www.kratikal.com

Malware attacks

Total cost of Malware vs new Malware

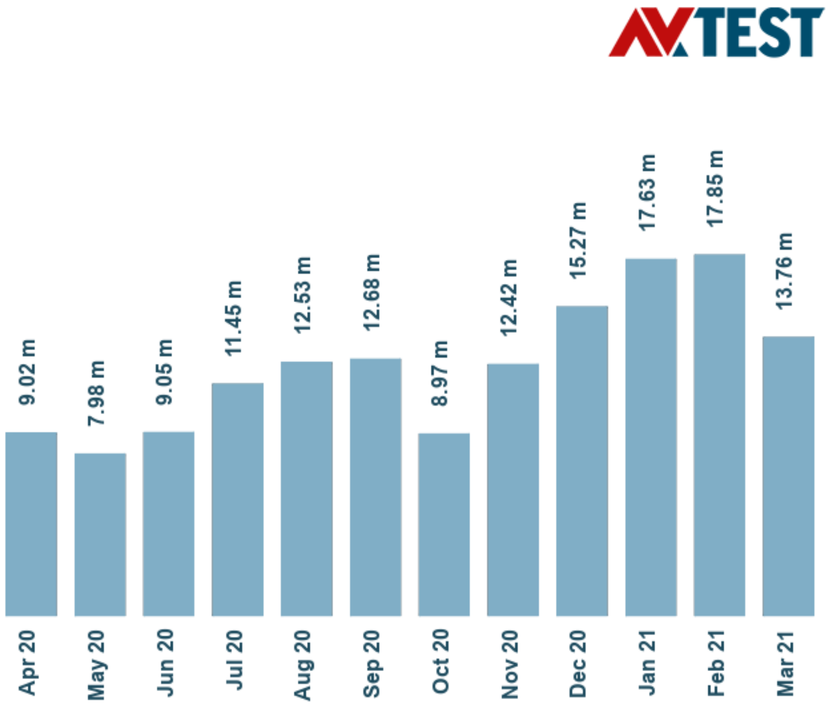
Total malware



Last update: March 22, 2021

Copyright © AV-TEST GmbH, www.av-test.org

New malware



Last update: March 22, 2021

Copyright © AV-TEST GmbH, www.av-test.org

Major cyber attacks and data breaches

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Most organisations struggled in 2020

51%

of organisations have suffered from a ransomware attack.

Source: *State of Email Cyber Security 2020 Report, Mimecast*

46%

report having cyber security breaches or attacks in the last 12 months.

Source: *Cyber Security Breaches Survey 2020*

85%

received little or no security training to help make informed business risk decisions and mitigate risk.

Source: *2020 Cyber Threat Intelligence Report*

52%

of all cyber attacks in March 2020 were finance-related

Source: *Carbon Black*

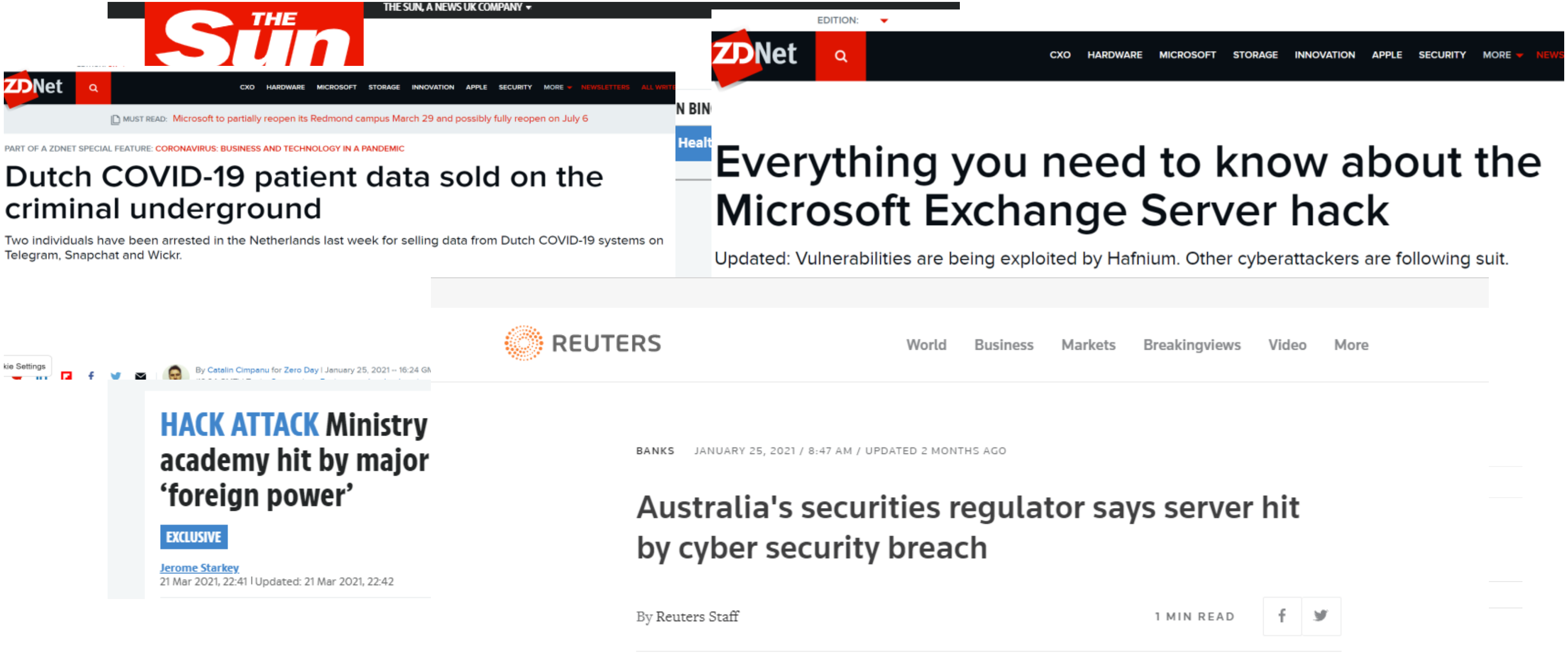
69%

have not changed the default password on their home Wi-Fi Router.

Source: *Proofpoint 2020 State of the Phish Report*

Major cyber attacks in 2021

In the headlines



THE SUN, A NEWS UK COMPANY
The Sun
ZDNet
CXO HARDWARE MICROSOFT STORAGE INNOVATION APPLE SECURITY MORE NEWSLETTERS ALL WRITE
EDITION:
ZDNet
CXO HARDWARE MICROSOFT STORAGE INNOVATION APPLE SECURITY MORE NEWS
REUTERS
World Business Markets Breakingviews Video More

MUST READ: Microsoft to partially reopen its Redmond campus March 29 and possibly fully reopen on July 6

PART OF A ZDNET SPECIAL FEATURE: CORONAVIRUS: BUSINESS AND TECHNOLOGY IN A PANDEMIC

Dutch COVID-19 patient data sold on the criminal underground

Two individuals have been arrested in the Netherlands last week for selling data from Dutch COVID-19 systems on Telegram, Snapchat and Wickr.

By Catalin Cimpanu for Zero Day | January 25, 2021 -- 16:24 GM

Everything you need to know about the Microsoft Exchange Server hack

Updated: Vulnerabilities are being exploited by Hafnium. Other cyberattackers are following suit.

HACK ATTACK Ministry academy hit by major 'foreign power'

EXCLUSIVE

Jerome Starkey
21 Mar 2021, 22:41 | Updated: 21 Mar 2021, 22:42

BANKS JANUARY 25, 2021 / 8:47 AM / UPDATED 2 MONTHS AGO

Australia's securities regulator says server hit by cyber security breach

By Reuters Staff 1 MIN READ

Headline data breaches in 2020/21

Examples

Blackbaud

Suffered a ransomware attack which affected educational institutions and charities in the UK, the US and Canada.

Spotify

Musicians had their Spotify pages defaced just a week after it suffered a credential stuffing attack which compromised over 300,000 accounts.

Twitter

In June, celebrity Twitter accounts were hacked, which resulted in 398 people being scammed out of more than £109,000 in Bitcoins.

T-Mobile

American telecommunications provider T-Mobile has disclosed a data breach after an unknown number of customers were apparently affected by SIM swap attacks.

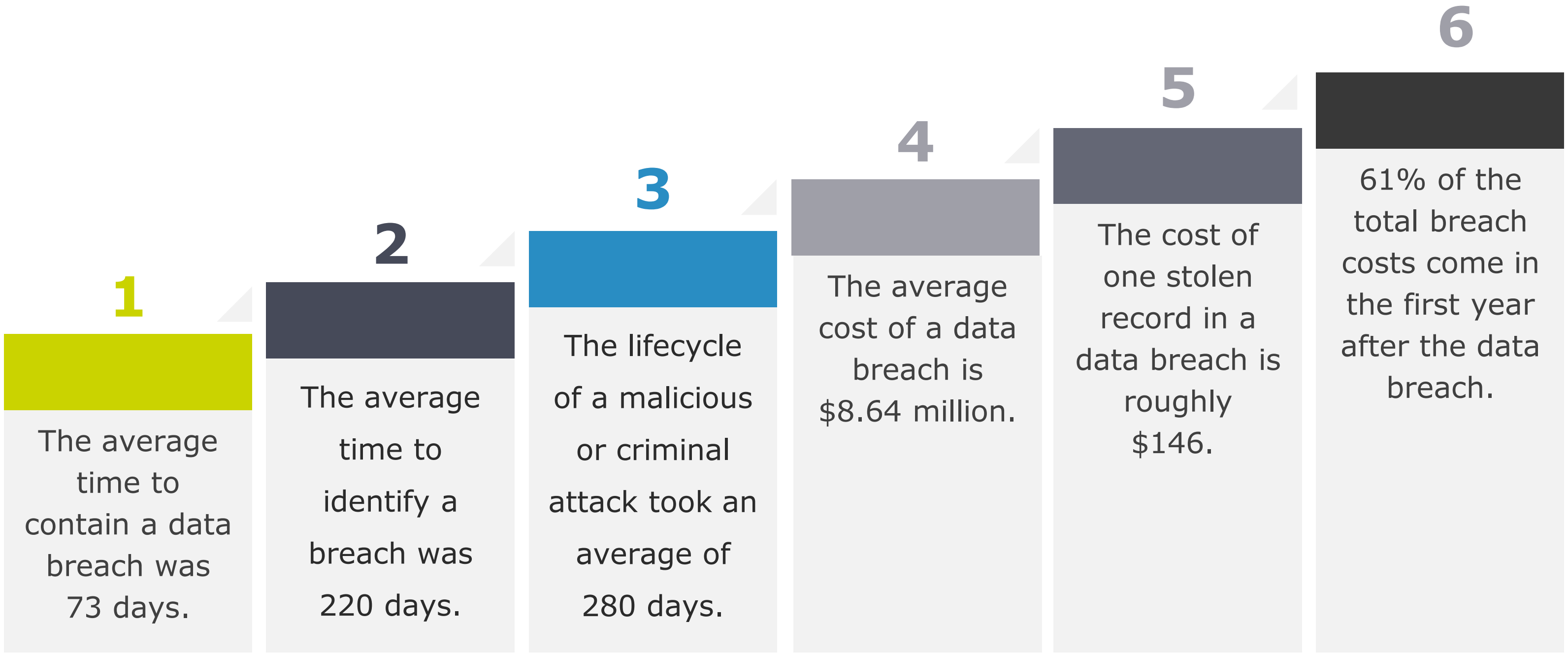
Foxtons Group

Under scrutiny for downplaying the severity of a cyber attack that has compromised the financial details of 16,000 customers.

Hackers Break Into 'Biochemical Systems' At **Oxford University Lab Studying Covid-19**

Key data about cyber breaches

IBM Data Breach Report 2020



1

The average time to contain a data breach was 73 days.

2

The average time to identify a breach was 220 days.

3

The lifecycle of a malicious or criminal attack took an average of 280 days.

4

The average cost of a data breach is $8.64 million.

5

The cost of one stolen record in a data breach is roughly $146.

6

61% of the total breach costs come in the first year after the data breach.

What about attacks on SMEs?

70% of cyberattacks target small businesses

43% of SMEs have no cyber security plan.

23% of SMEs have no endpoint security.

32% of SMEs rely on free, consumer-grade cyber security software.

58% of SMEs think they’re not a target for cyber attacks.

Reality: SMEs are under-protected, under-resourced and are easy targets!

Phishing and stolen credentials the top risks for SMEs.

Unpatched vulnerabilities make for easy targeting.

RUSI: Cyber Fraud and ‘Silent Stealing’

Cyber security and Privacy:
Two Sides of the Same Coin

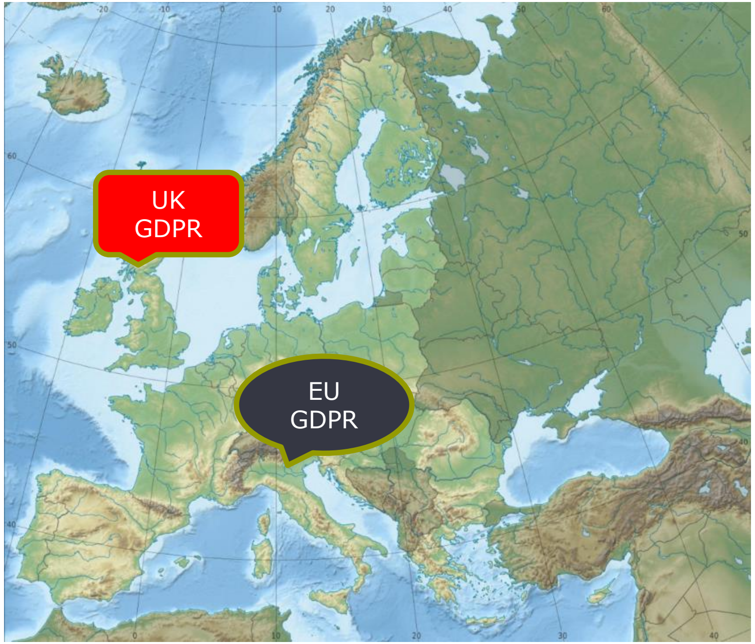
governance

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Post Brexit, GDPR becomes two.

Which means?



UK is a **Third Party** to **the EU –** and **vice versa**

Trading into the EU requires compliance with both legal frameworks.

Trading internationally may have other privacy compliance requirements

Fines – up to 4% of global revenue – could be levied under both laws!

Cyber and privacy

Data protection due diligence and planning now part of deal prep.

Privacy

- Lawful basis for processing personal data?
- Legitimate interest tests?
- DPIAs?
- Special categories of data?
- Customer acquisition, email marketing lists (Articles 13 and 14)

Cyber security

- Penetration tests.
- Access and authorisation policies.
- History of breaches and incidents.
- Continuity plans.
- Certifications – Cyber Essentials, ISO 27001, Sector-specific (eg HIPAA)

The Board and Senior Managers: Managing cyber exposure

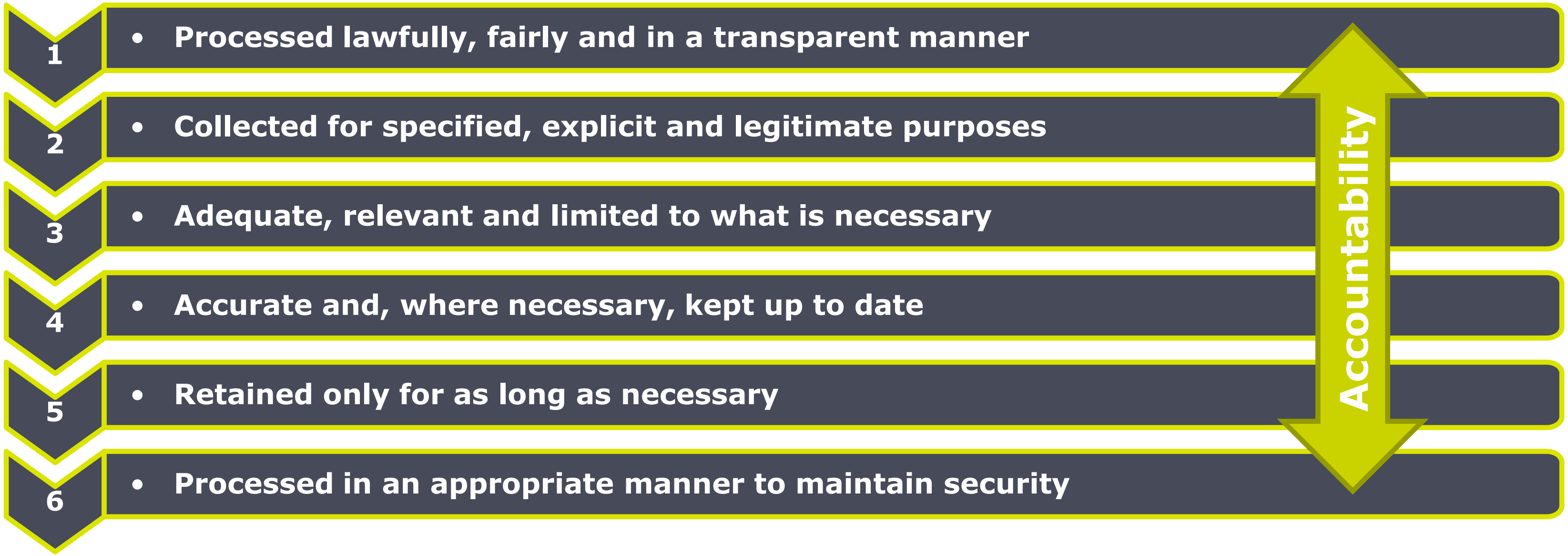
Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Accountability under GDPR

What it means for the Board and Directors

- Article 5: *Principles relating to processing of personal data*
- “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). “



1 • Processed lawfully, fairly and in a transparent manner

2 • Collected for specified, explicit and legitimate purposes

3 • Adequate, relevant and limited to what is necessary

4 • Accurate and, where necessary, kept up to date

5 • Retained only for as long as necessary

6 • Processed in an appropriate manner to maintain security

Copyright © IT Governance Limited | US | EU v0.1 | Classification: [Restricted/ Confidential/ Client Confidential/ Public]

Application of the principle of accountability

What it means for the Board and Directors

Governance: Board accountability	Corporate risk register Monthly/quarterly reports on compliance and incidents	
	Nominated responsible director	
Clear roles and responsibilities	Data Protection Officer Head of Cyber Security	
Compliance Framework	PIMS/ISMS	
	Cyber incident response	
	Cyber Essentials a minimum security standard	
	Certification and data seals (Article 42) – ISO 27001	
Data Protection by Design and by Default	Data Flow Audits Penetration testing ISMS Audits	
	Data Protection Impact Assessments (DPIA) and Risk Assessments	‘Apply technical and organisational measures’ ‘Taking account of the State of the Art’

Practical steps: what you should do now

Cyber and privacy risks co-exist. Attackers are sophisticated. Regulators and customers are unforgiving. Any organisation with assets is a target. You have to act before you are breached.

Recognise the extent of your risk

- Cyber and privacy risks co-exist. Attackers are sophisticated. Regulators and customers are unforgiving. Any organisation with assets is a target. You have to act before you are breached.

Put a cyber security and privacy strategy in place

- Once you have accepted that there is a risk, put in place a cyber security and privacy strategy. If you don’t have the resources internally to manage this, it is likely to be possible to outsource it and use the skills of expert professionals.

Update your privacy posture

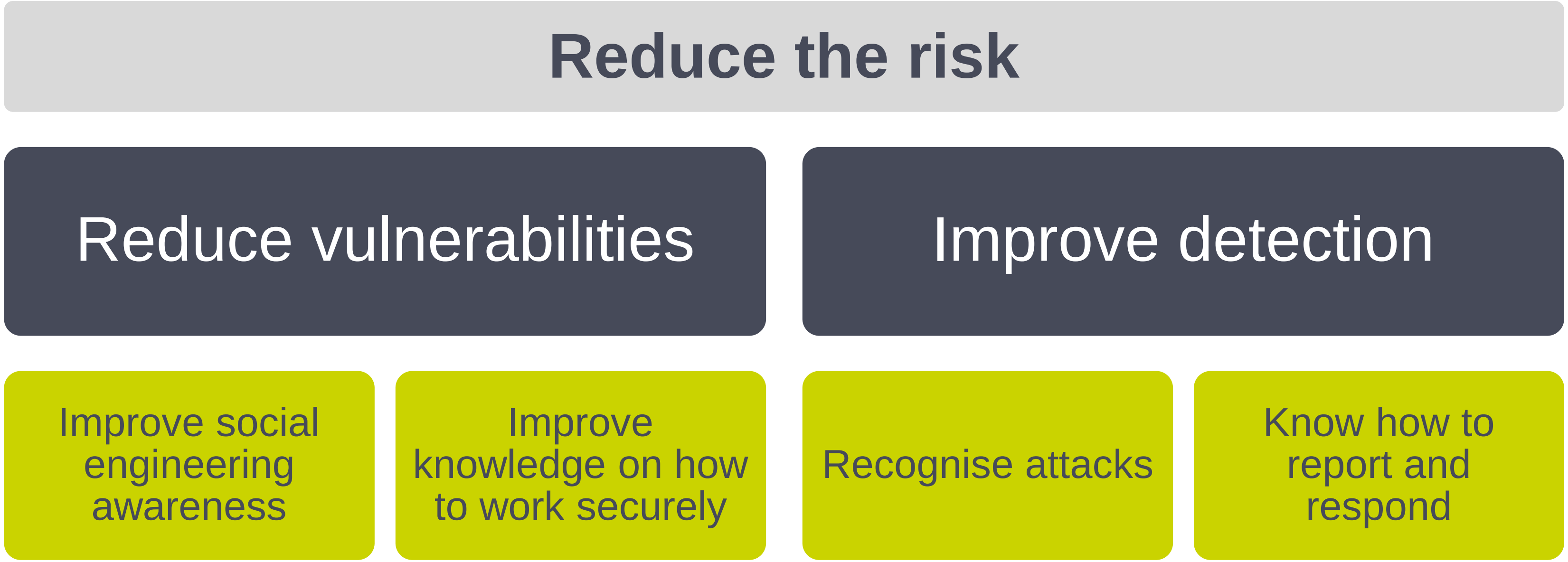
- Adapt your documentation to UK GDPR and put in place appropriate processes for all extra-UK data flows.

Train your staff

- All staff need to understand the new privacy and data protection laws, as well as being able to spot phishing and BEC attacks.

Staff awareness programmes

The human firewall to prevent cyber attacks and data breaches



Reduce the risk

Reduce vulnerabilities

Improve detection

Improve social engineering awareness

Improve knowledge on how to work securely

Recognise attacks

Know how to report and respond

Thank you

Our Expertise,
Your Peace of Mind

Protect • Comply • Thrive

Contact us

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

Like us on Facebook
/ITGovernanceLtd

Follow us on Twitter
/itgovernance