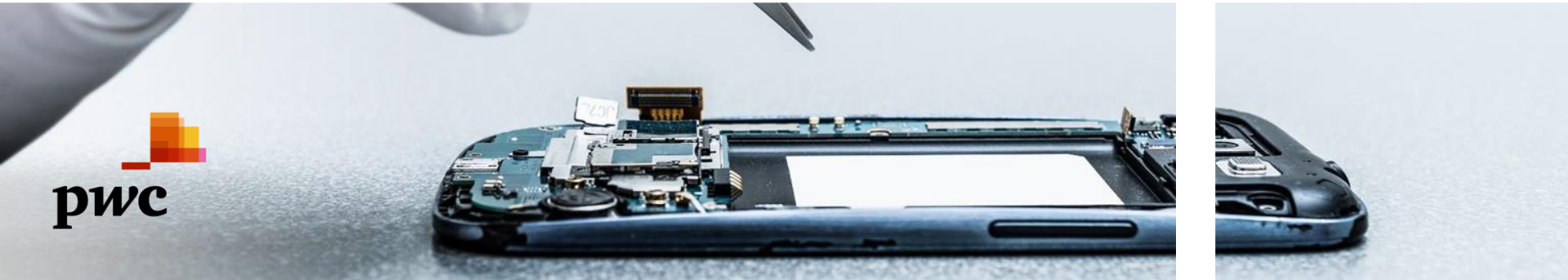
Auditing cybersecurity

ISACA
Chris Potter and Analia Millet - PwC
16 March 2021



1

Cybersecurity in the post-COVID world

Security breaches common in UK businesses

https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

46%

Of UK businesses had a security **breach** in the last 12 months

75%

Of **large** UK businesses had a security breach in the last 12 months

32%

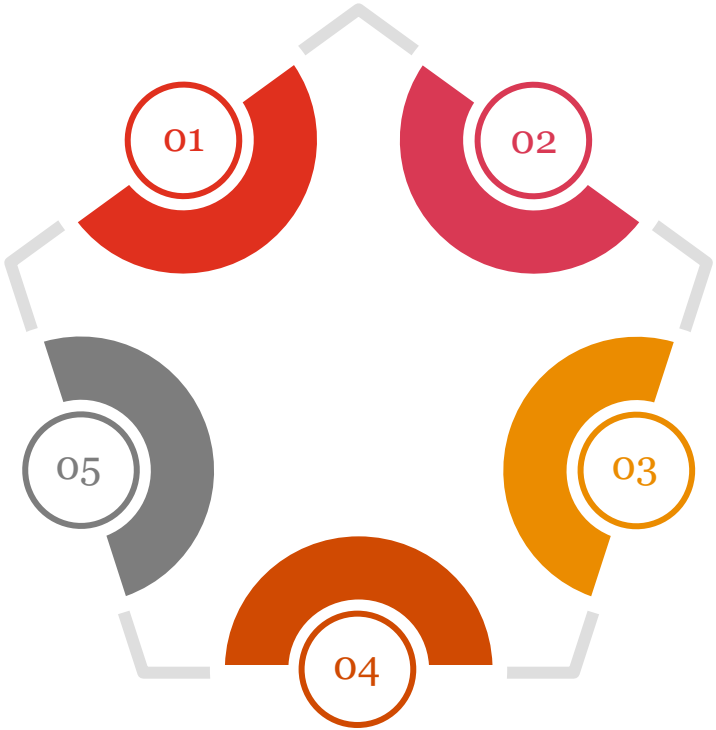
Experience attacks or breaches at least **once a week** (up from 22% in 2017)

86%

Of those attacked experienced **phishing** attacks (up from 72% in 2017), whereas viruses and malware less common than in 2017

Infosecurity magazine - State of cybersecurity report 2020

https://www.infosecurity-magazine.com/white-papers/state-of-cybersecurity-report-2020/



01 Impact of Covid-19

"Companies strained to quickly enable remote working securely"
"Can leave doors open and create a massive attack surface"
Cyberattacks against healthcare sector up by 150% (e.g. phishing using WHO)

02 The Cloud

Very few modern businesses are not working in the cloud
Increasing use of cloud based solutions to meet remote working needs
Need "to focus on solutions that secure the cloud"

03 Artificial intelligence and machine learning

"As the use of AI to develop autonomous and semi-autonomous systems grows, so too must the understanding of the human-AI interface"
It's now the norm for companies to automate "routine, time-consuming tasks"
Adversarial machine learning being used in attacks

04 The human element

Increased recognition of the profession of cybersecurity
Ongoing shortage of cybersecurity skills
"Emails being sent accidentally cause data breaches"
Need to move from training to embedding security in day to day practice

05 Phishing

In any crisis, "we see an increase in the number of phishing attacks"
"Alarmingly high success rate, yet a relatively low detection rate"

Ransomware and data poisoning increase since lockdown

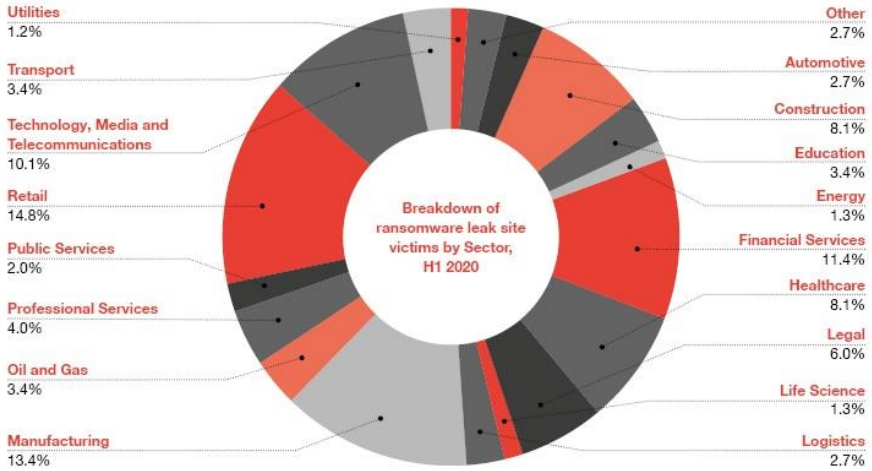
https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html

December 2019: Actors controlling Sodinokibi ransomware post links to the data stolen by it on a private, Russian-speaking dark web forum.

January 2020: Semi-public site posts stolen data gathered using Maze ransomware.

Since then, nine further ransomware actors have created their own leak sites and we expect additional actors to do the same.

By 20 May, over 150 organisations globally have had their data published on leak sites; the majority of these (60%) have occurred after 11 March, when the WHO first declared the COVID-19 outbreak to be a pandemic.



Five security breaches of note in the last year

Travelex (January 2020)

- Sodinikibi ransomware attack on 31 December 2019 - company forced to take down its websites across 30 countries. Many still offline two weeks later.
- Caused service interruption in more than a dozen UK banks.
- Travelex went into administration in August 2020.

Marriott (March 2020)

- Marriott disclosed a security breach that impacted the data of more than **5.2 million** hotel guests who used their company's loyalty application.
- Hackers obtained login credentials of two accounts of Marriott employees who had access to customer loyalty scheme information. Data was siphoned off for a month before the breach was discovered.

.

Zoom credentials for sale (April 2020)

- Zoom application became vulnerable to various security threats and eventually became a victim of a data breach.
- 500,000 stolen Zoom passwords allegedly available for sale in dark web crime forums.

Twitter (15 July 2020)

- Hackers hijacked Twitter accounts of high profile US personalities like Barack Obama, Elon Musk, Joseph R. Biden Jr., Bill Gates, and many more.
- Hackers posted fake tweets from these accounts, offering to send $2000 for $1000 sent to an unknown Bitcoin address.

Solarwinds (December 2020)

- Hackers infiltrate Solarwinds in September 2019 and plant SUNBURST malicious code (with a backdoor) into automatic updates for its Orion IT management software between March and June 2020.
- 18,000 organisations (including US agencies, Microsoft, FireEye, Intel, Cisco and Deloitte) were affected.

How do most attacks happen?

Phishing is an organised crime exploiting human emotions

Fear/Worry

WHO (Covid-19)

Invoice needs paying

Greed

Headhunters

Free coffee

Black Friday sales

Anger

Wi-fi going down

Spear-phishing

65% of attacking groups use social media data on target (and their family) to personalise their attacks (Symantec 2019)

2

Auditing cybersecurity

“More than three-quarters of executives in our Global Digital Trust Insights 2021 survey say that “assessments and testing, done right, can help them target their cybersecurity investments.”

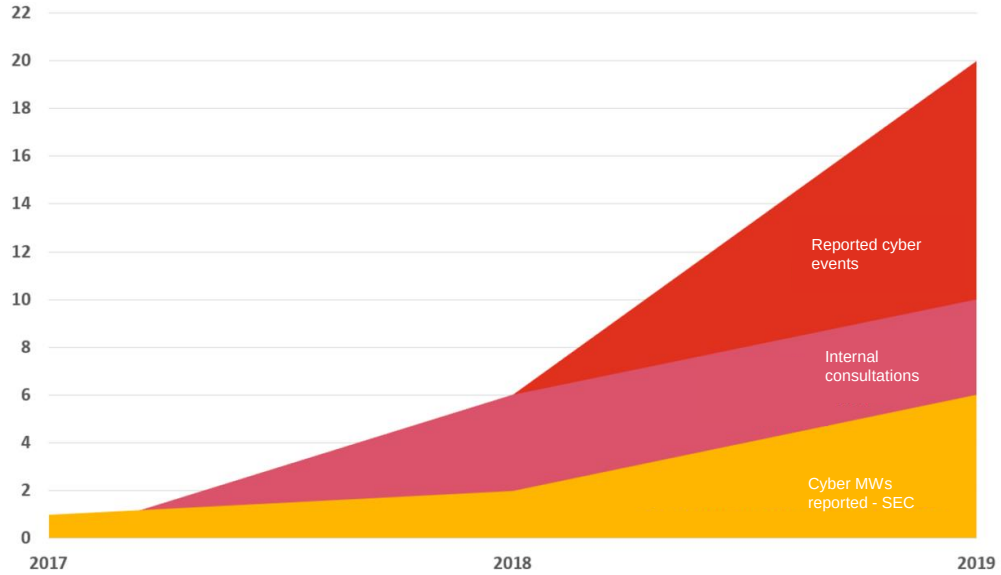
Auditing cyber

1. An evolving risk
2. Cybersecurity risk in the audit
3. Audit response to a cyber incident
4. Things to take away

1

An evolving risk

An evolving risk



Cyber events continue to rise, requiring increased involvement by the auditors in the evaluation of the impact to registrants; financial statements and ICFR

2020 has seen a huge increase in ransomware attacks. The transition to a remote workforce as a result of the COVID-19 pandemic has increased the attack area while simultaneously limiting the effectiveness of cyber defenses.

Continued focus from the SEC and PCAOB

The SEC and PCAOB continue to highlight cybersecurity as a topic of focus in inspection / exam outlooks as well as speeches and statements

SEC's Office of Compliance Inspections and Examinations

In January 2020 the SEC's OCIE released its Cybersecurity and Resiliency Observations to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency.

"The seriousness of the threats and the potential consequences to investors, issuers, and other securities market participants, and the financial markets and economy more generally, are significant and increasing. As markets, market participants and their vendors have increasingly relied on technology, including digital connections and systems, cybersecurity risk management has become essential."

PCAOB speech on Cybersecurity

In an October 2019 speech entitled "keep Calm and Carry On: The Role of Regulators in Cybersecurity and Resiliency" PCAOB shared perspectives on the continued increase of cyber threats in today's environment and highlighted baseline protections and best practices related to basic cyber hygiene:

- Multi-factor authentication
- Limiting special, high level data and system access
- Patch management
- System scanning for malicious activity
- segregation of critical systems and data

2

Cyber risk in the audit

Cyber risk in the audit

Internal auditors:
Informing the board and executive management about how effectively the organisation assesses and manages its cyber risks

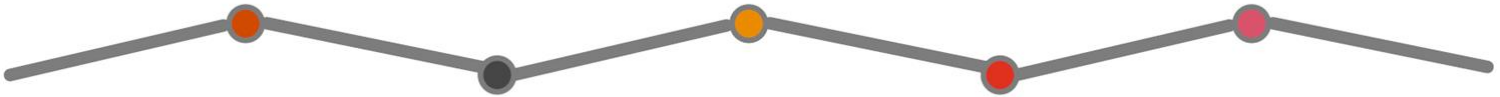
External auditors:
Considerations related to cyber risk include the potential impact on the financial statements, ICFR and the ability of an organisation to report on a timely basis.

Cyber risk in the audit

Assess the **inherent risk** of cybersecurity - what are the aspects of the entity's business and operations that give rise to cybersecurity risk

Assess each of the **common exposures** and determine whether there **is risk of material misstatement**

Perform testing of identified control(s) and evaluate the impact of identified deficiencies, if any



Understand **how the entity manages cybersecurity risk** as part of its overall risk management program

For each exposure, **add the corresponding risk and control OR document rationale** for why the exposure does not present a risk of material misstatement

Striking the right balance between providing a view of cyber capabilities and avoiding a false sense of security

Cyber risk in the audit

Scope

- **Clearly define the boundaries of the audit subject**
- **Understand the critical dependencies**
- **Manage expectations: what is the objective of the audit?**
- **Exclusions need to be carefully considered**

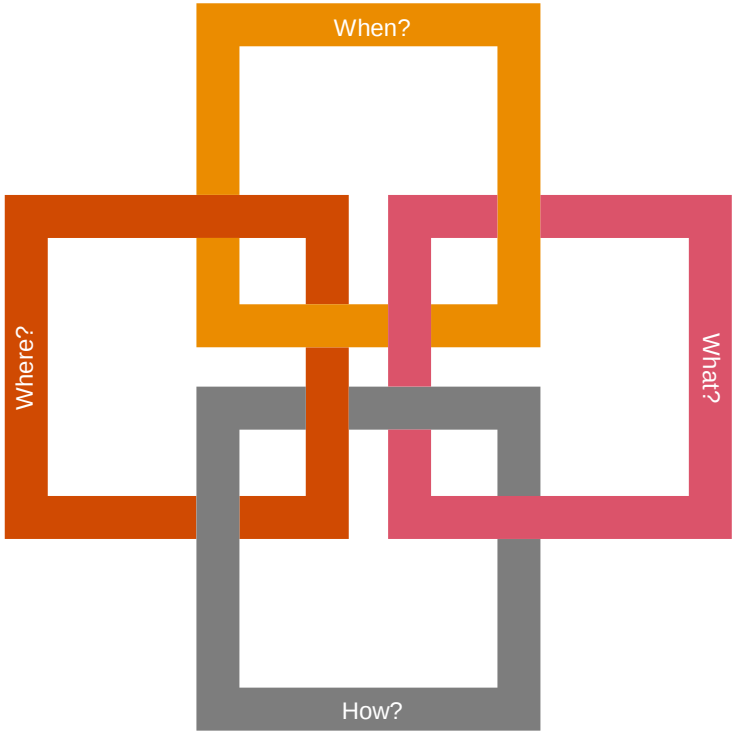
Risk

- **Risk of material misstatement**
- **Management’s cyber risk assessment and our risk assessment**
- **Typical risk areas should be considered**

3

Audit response to a cyber incident

Responding to a cyber incident



What?
Nature of attack, objective, what data was compromised.
What steps were taken to control the breach and respond
What has been communicated internally and to the market / authorities

When?
When did the attacker gain access?
When did their reveal their presence in the network
Timing between the incident happening, management's identification and response

Where?
Which servers, databases, applications?
Which entities / businesses / countries / geographies?
Compromised operations

How?
What was the vulnerability that was exploited to access the systems?
How did management learn of the incident?
Have management engaged cyber experts / legal counsel?
How did management determine whether the incident represents a financial risk

Questions and answers

Thank you

pwc.com