Cyber security: Protect your retail business

RETAIL COMMUNITY WEBINAR

HOSTED BY RICHARD ANNING, HEAD OF TECH FACULTY, ICAEW

Cyber Security Protect Your Retail Business

ICAEW Webinar 10 March 2020
George Quigley

FOULKON
DECODING TECHNOLOGY RISK

+44 (0) 330 002 0900 foulkon.com enquiries@foulkon.com

Cyber Security Risk

Retail Context

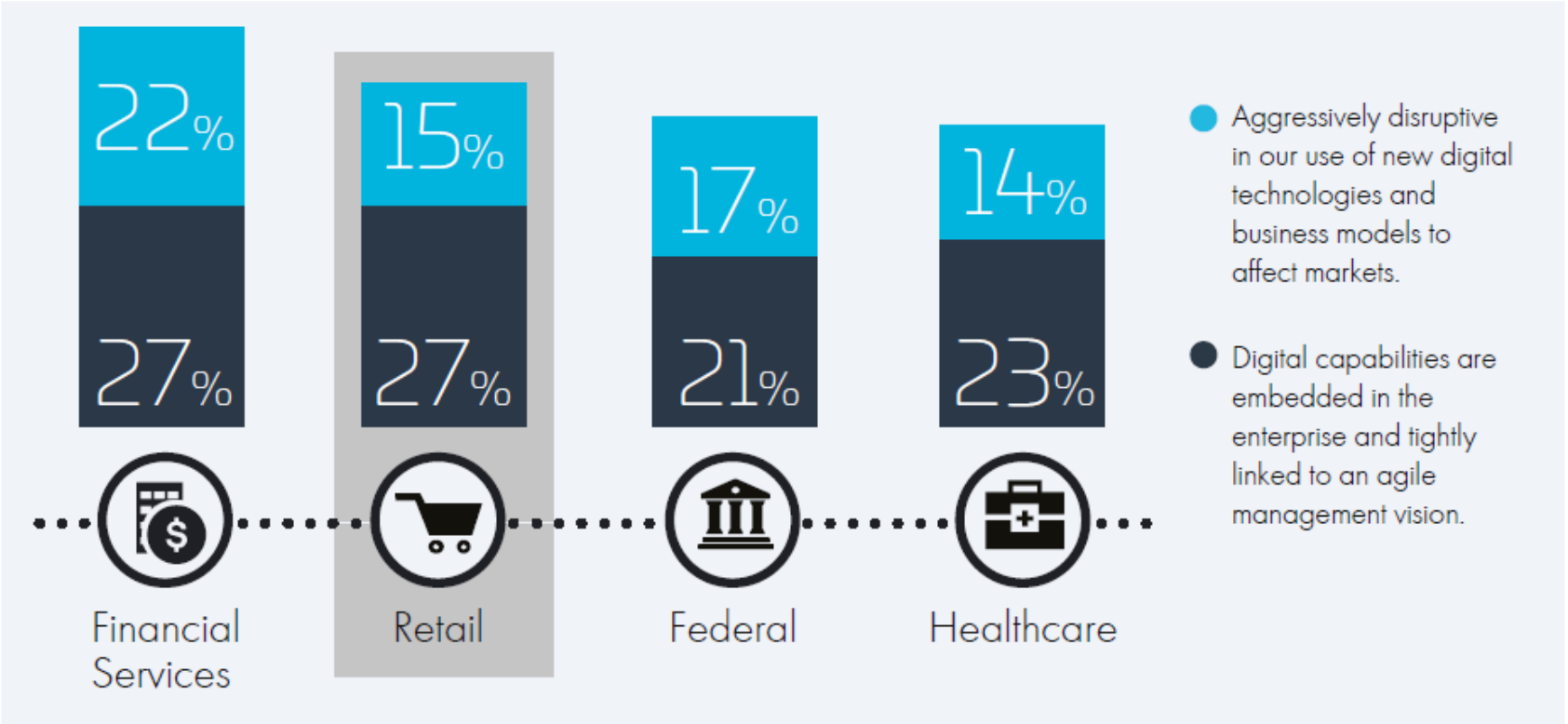


Figure 1 – Digital transformation stance
Source: 2019 Thales Data Threat Report Survey, IDC, November, 2018

Retail Context

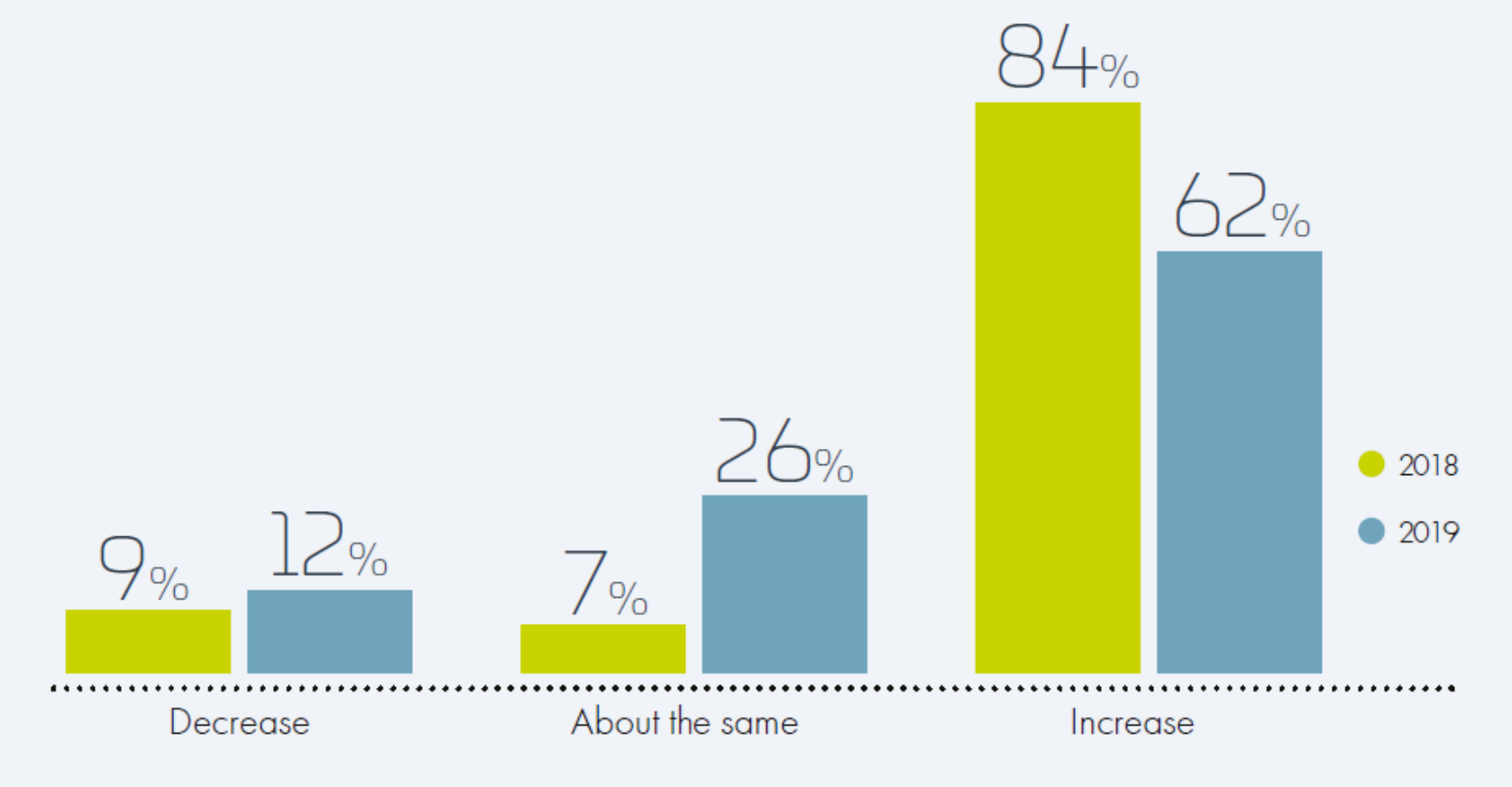


Figure 2 – IT security spend in U.S. retailers
Source: 2019 Thales Data Threat Report Survey, IDC, November, 2018

Retail Context

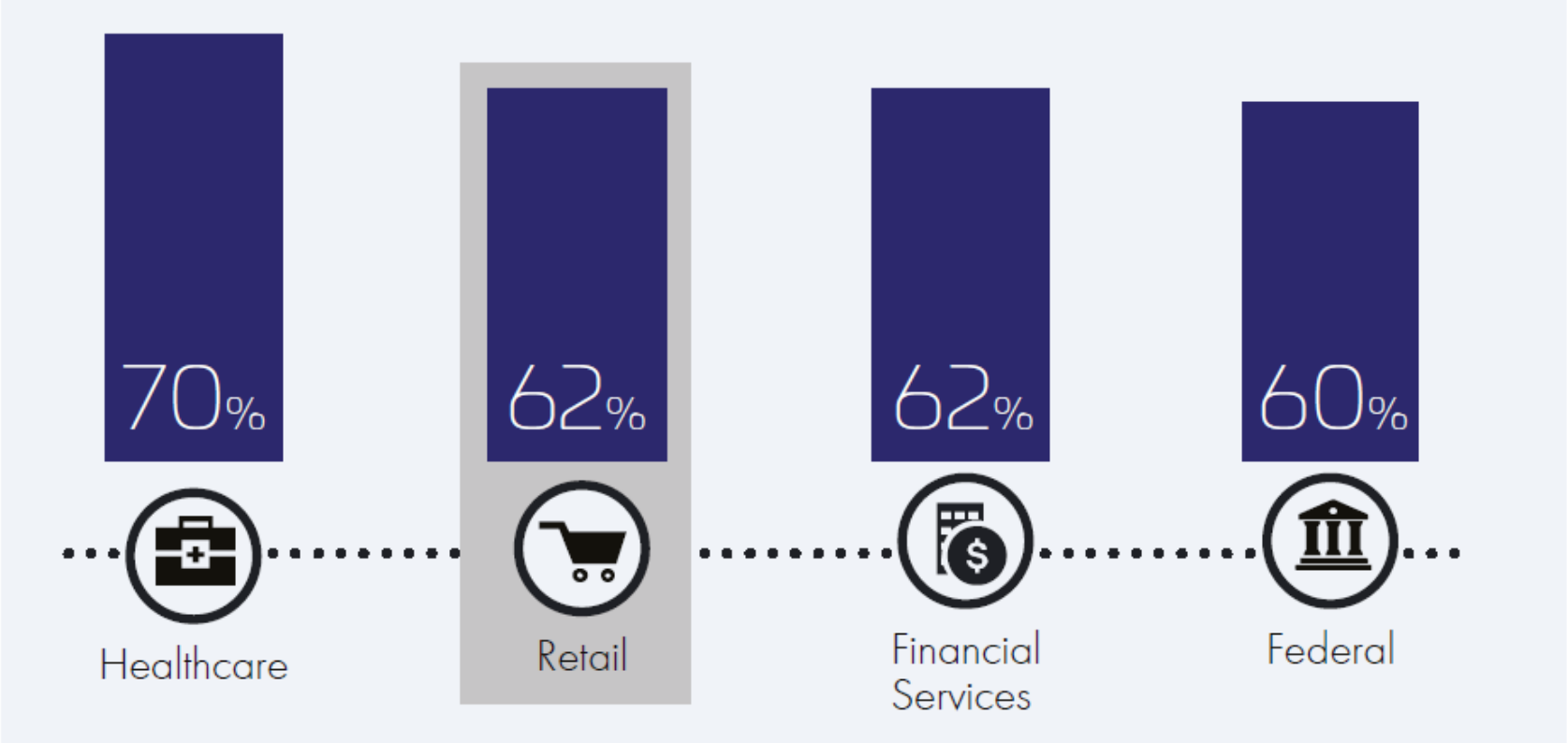


Figure 3 – Breach incident rates (at any time)
Source: 2019 Thales Data Threat Report Survey, IDC, November, 2018

Retail Context

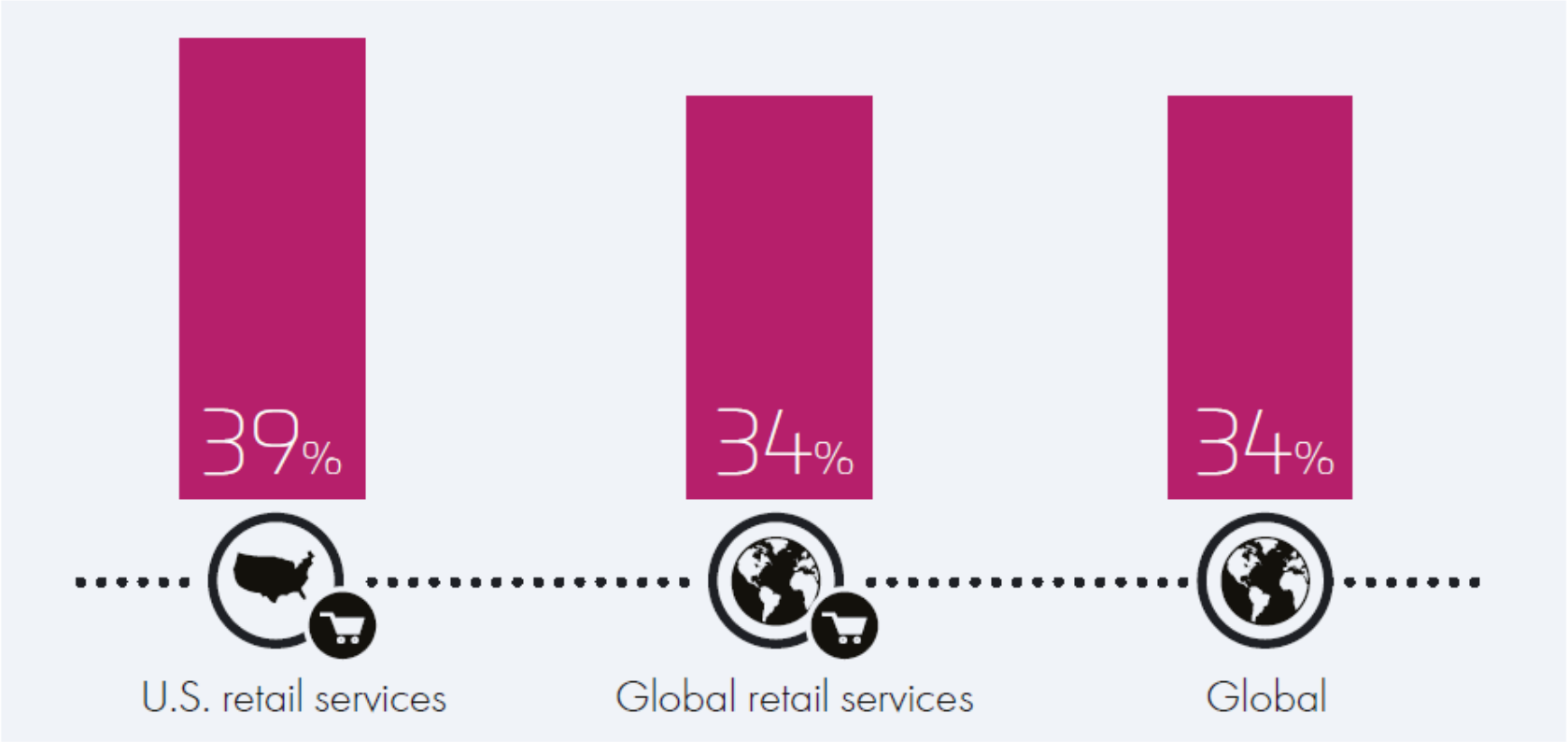


Figure 4 – Vulnerable/very vulnerable to security threats (U.S.)
Source: 2019 Thales Data Threat Report Survey, IDC, November, 2018

Retail Context

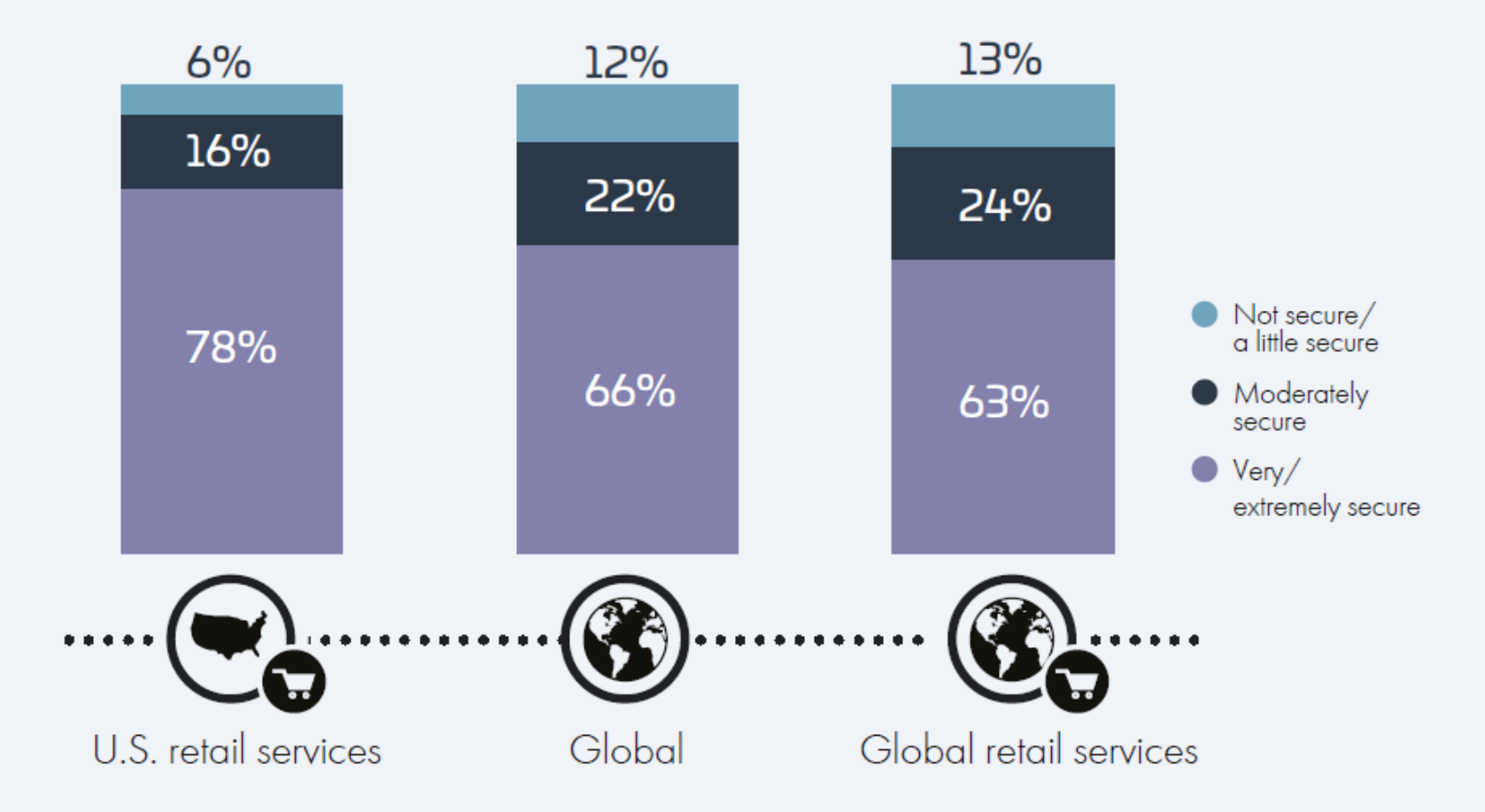


Figure 6 – Security level of new technology deployments
Source: 2019 Thales Data Threat Report Survey, IDC, November, 2018

Retail Context

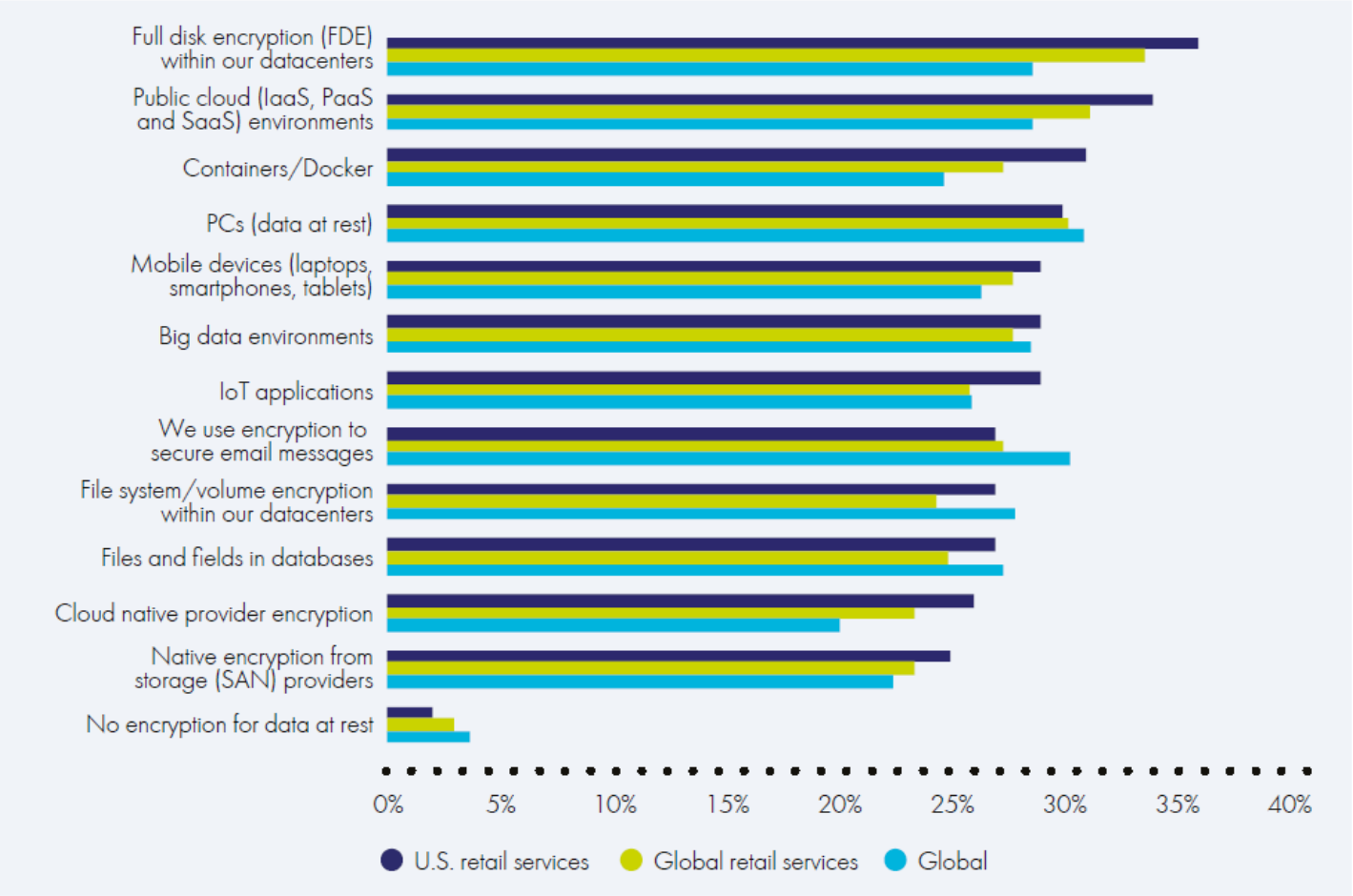


Figure 14 – Encryption use rates
Source: 2019 Thales Data Threat Report Survey, IDC, November, 2018

Case Study - Evolving Attacks

CarPhone Warehouse – 2015 Breach

Systems Affected – websites including (e-commerce)

What Happened?

1. Attacker scanned the websites using Nikto (open source freely available web security scanning tool)
2. The scan revealed a vulnerable WordPress CMS. It was considerably out of date, contained several vulnerabilities and was accessible from the Internet
3. The attacker installed “web shells” giving file management and database functionality to the attacker
4. The attacker found credentials and other information in “plain text” (not encrypted), which were used to further the attack
5. The attacker viewed significant amounts of data and extracted a large file or files out of the network

DSG Retail – 2018 Breach

Systems Affected - DSG’s computer system

What Happened?

1. Attacker compromised the DSG infrastructure
2. Attacker gained control of multiple domain administrator credentials
3. Attacker installed malware on POS systems at Currys PC World and Dixons Travel Stores
4. Significant amount of SQL database reconnaissance and data theft appeared to have taken place
5. Personal data appears to have been exfiltrated along with credit card information

Case Study - Evolving Attacks

CarPhone Warehouse - ICO Notice 2018

Timeframe

21 July to 5 August 2015

Commissioners View

1. Out of date software in use (6 years old)
2. Software patching seriously inadequate
3. Inadequate Vulnerability Scanning and Penetration Testing
4. No Web Application Firewall in use
5. No Anti Virus in use
6. Inadequate monitoring
7. Shared Passwords
8. Inappropriate data retention
9. Poor encryption security

DSG Retail – ICO Notice 2020

Timeframe

24 July 2017 to 25 April 2018

Commissioners View

1. Insufficient network segmentation (related to POS)
2. Software patching of domain controllers and systems used to administrate them was inadequate
3. Vulnerability Scanning not performed on a regular basis
4. Failure to manage application whitelisting across all POS terminals
5. Logging and monitoring not adequate
6. POS system out of date
7. Failure to effectively manage domain administrator accounts
8. Failure to implement standard “hardened” builds

Case Study - Evolving Attacks

Ticketmaster, British Airways, et al Breaches

Known as Magecart attacks

A confederation of credit card skimmers that have been operating for a considerable period of time. They attack e-commerce sites to steal credit card information using a technique known as “form jacking”

How do they operate?

1. Magecart look for vulnerabilities in common e-commerce platforms
2. They use those vulnerabilities to access sites and insert themselves into the payment stream
3. The scripts they insert capture information as it is entered in real time
4. The scripts are able to capture all credit card information including CVV
5. There has been some recent evidence that they are also using the technique in order to attempt to gain login credentials

Who do they target?

Historically larger retailers. There is evidence that they are now targeting smaller luxury retailers that are likely to have higher value credit cards and smaller retailers that are less likely to notice their activities.

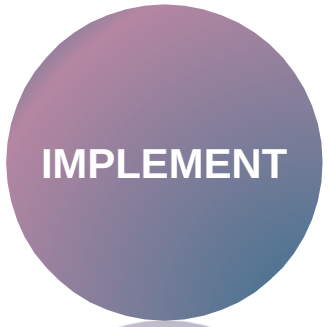
Managing Cyber Risk

Understand your specific cyber risks based on your business context, considering people, process and technology

Drives a cost effective solution

Assess whether your specific cyber risks are being managed properly in line with your risk appetite

Drives a practical approach



Remediation activities to bring your cyber risk in line with your risk appetite

Drives a pragmatic approach

Monitor context and assess your cyber risk and controls on an ongoing basis – go beyond compliance

Puts you in control

Contacts

George Quigley
Director,
Cyber Security & Data Privacy

+44 7973 311836
george.quigley@foulkon.com

David Styles CIPP/E
Director,
Cyber Security & Data Privacy

+44 7720 291222
david.styles@foulkon.com

Bluefin Professions

CYBER INSURANCE

Jeremy Goodacre
Head of Sales and Proposition, MARSH

ICAEW MEMBER REWARDS PARTNER

WHAT IS CYBER INSURANCE?

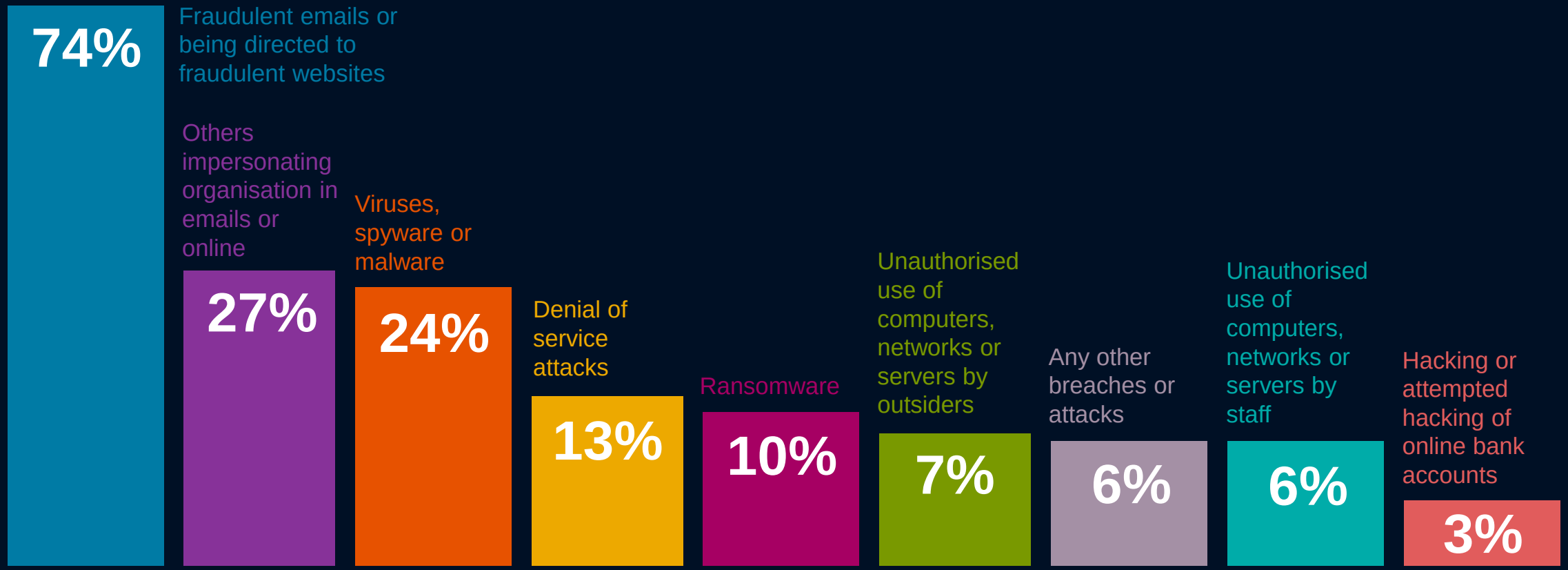
- Traditional property insurances only cover “physical damage.”
- Cyber insurance covers damage to digital/electronic assets without the requirement for physical damage to have occurred.
- Business interruption (BI) policies will only operate in the event of a claim from the same event of physical damage.
- BI policies won’t cover losses from business interruption arising from damage to your systems not involving physical damage.
- Liability, professional indemnity and crime policies often include elements of cyber cover. They can also contain exclusions and may not dovetail elegantly.

COVER OVERLAP

- Crime insurance.
- Professional indemnity insurance.
- Cyber insurance.
- Directors and officers insurance.

RISK WEIGHTING

TYPES OF BREACHES OR ATTACKS SUFFERED IN THE LAST 12 MONTHS



Basis: Organisations that identified a breach or attack in the last 12 months.

WHAT IS THE IMPACT OF A BREACH / ATTACK?

- In the event of a data breach you may:
  - Incur costs to notify the ICO and effected customers.
  - Incur costs in investigating the breach and rectify the issue.
  - Suffer adverse PR - 71% of customers would leave an organisation after a data breach*.
- However – it's not just about data!
  - Disruption and costs from downtime reach beyond data loss.
  - The focus has shifted to resilience (recovery from breach) and business interruption - 98% of businesses rely on digital communication or services*.
  - Cyber crime is by far the predominant issue currently**.

*HM Government: Cyber Security Breaches Survey 2018
**Edelman Privacy Risk Index

CYBER CRIME ON THE RISE

- Cyber crime is an increasing trend with 3 in 5 SMEs reporting an attack in the past 12 months.
- The Association of British Insurers (ABI) report just 11% of businesses have a cyber insurance policy.
- A cyber policy can respond in different ways:
  - Reimburse you for loss resulting from fraudulent use of data in your computer system.
  - Payments due to your telephone service provider resulting from hacking.
  - The cost of responding and payment of ransom demands if you are the victim of crime.

Bluefin Professions

ICAEW MEMBER REWARDS PARTNER

CYBER INSURANCE - A WELL KEPT SECRET?

- 74% of businesses consider cyber security as a high priority.
- Just 9% of businesses have explicit cyber cover. Compares to 30% in the US.
- Half of the business leaders interviewed (1,519) were not aware of the existence of cyber insurance.
- The balance did not consider their businesses were at sufficient risk.
- Those responsible for cyber security are often not the same individuals who will make decisions about insurance - so there's a disconnect.

*HM Government: Cyber Security Breaches Survey 2018

IT'S NOT JUST ABOUT THE POLICY COVER

CYBER INSURANCE AS A RISK MANAGEMENT TOOL

- **Time is of the essence** when it comes to responding to an incident
- **Only 21% of businesses** have a formal cyber security incident management process
- **Cyber policies provide** a panel of legal accountancy, forensic IT and public relation specialists (initial response < 1 hour)

- **This structure enables rapid, expert response** to effectively manage an incident, especially in the first 72 hours – the Critical Response Time
- **Policies also provide:**
  - Notification letters, call centre, credit monitoring service
  - Reputational risk management is key
  - Major component in increasing the relevance of cyber insurance

*HM Government: Cyber Security Breaches Survey 2018

Bluefin Professions

ICAEW MEMBER REWARDS PARTNER

SCENARIO 1 - PHISHING

Losses	PI Policy	Cyber Policy
1. Payment to HMRC: £300,000	**£nil** Example of a 1st party loss and so cover not available However, if payment had been made to HMRC using client funds and a claim was made by this client then this would be covered.	**£300,000** Cover is available for fraudulent impersonation (social engineering).
2. Forensic investigation costs to ascertain how breach occurred and to prevent future event. £50,000	**£nil** Own expense/costs (1st party)	**£50,000** Would be met by Cyber Policy
Total £350,000	**£nil to £300,000**	**£350,000**

SCENARIO 2 - RANSOMWARE / MALWARE

Losses	PI Policy	Cyber Policy
1. Ransom Sum **£1,500,000**	**£nil** Example of a 1st party loss and so cover not available	**£1,500,000** 1st party losses covered
2. Loss of service/business interruption **£500,000**	**£nil** No 1st party losses will be paid	**£500,000** Loss of trade/business income capable of cover under a cyber policy. Method for calculating the trading losses will be set out in advance within the policy
3. Forensic investigation costs to ascertain how breach occurred and how to prevent future events. **£50,000**	**£nil**	**£50,000** 1st party losses covered

WHAT INFORMATION IS NEEDED FOR A QUOTE?

- **Basic information required to obtain a quotation:**
  - **Turnover**
  - **Wage roll**
  - **Number of client records held**
- **Do you have a website and what would be the detriment to your business if this site was shut down.**
- **What protection does your business have? Firewall, anti-virus etc.**
- **Do you regularly back up your data? Cloud/hard drive etc.**
- **Call Marsh Commercial/Bluefin Professions.**
- **CYRISQ**

Bluefin Professions

ICAEW MEMBER REWARDS PARTNER

Bluefin Professions

ICAEW MEMBER REWARDS PARTNER

Questions?

icaew.com