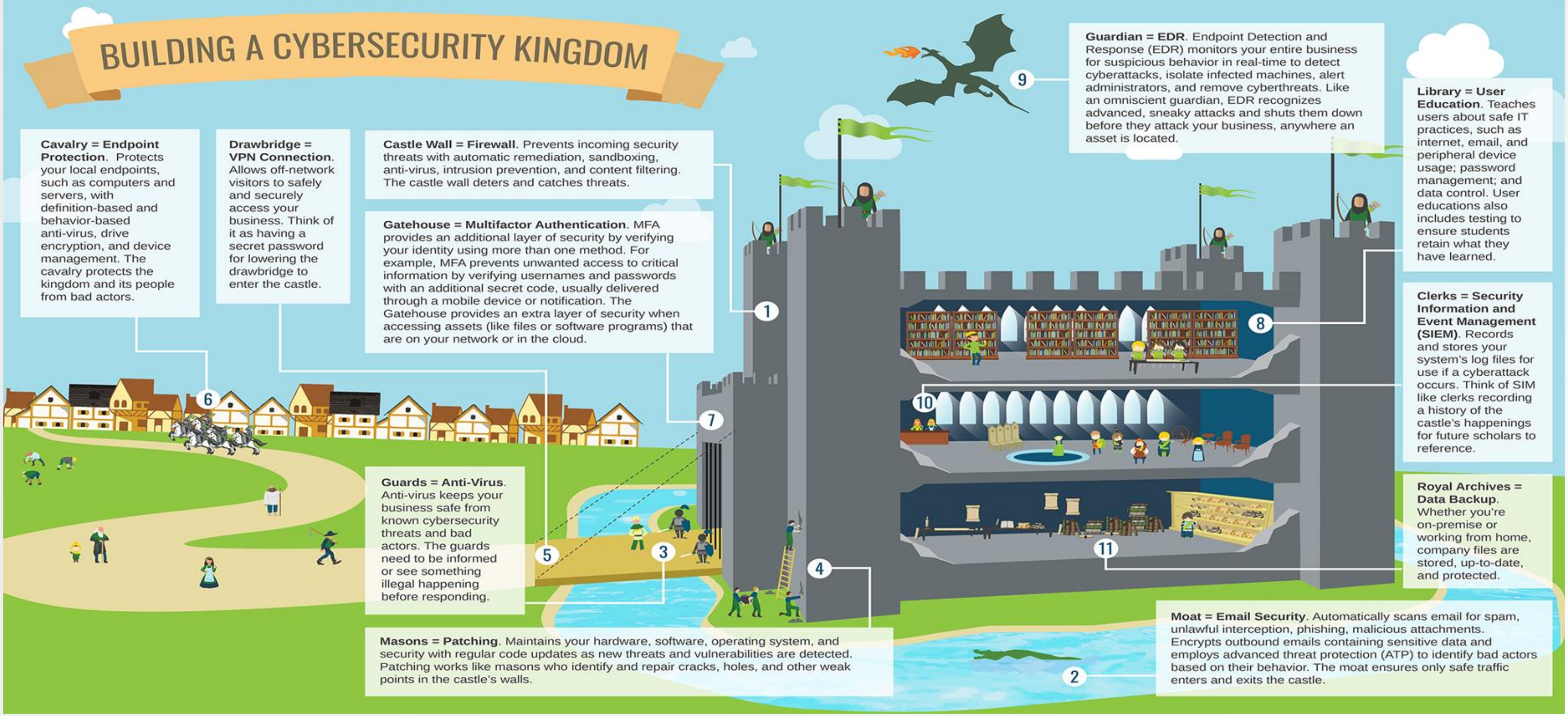
The pathway towards, and need for Digital Trust?

Mark Brown
Global Managing Director
Digital Trust Consulting
British Standards Institution (BSI)

By Royal Charter

Is cybersecurity an impossible nirvana, and is cyber resilience the new target operating model?

Traditional approaches to Cybersecurity



Cavalry = Endpoint Protection. Protects your local endpoints, such as computers and servers, with definition-based and behavior-based anti-virus, drive encryption, and device management. The cavalry protects the kingdom and its people from bad actors.

Drawbridge = VPN Connection. Allows off-network visitors to safely and securely access your business. Think of it as having a secret password for lowering the drawbridge to enter the castle.

Castle Wall = Firewall. Prevents incoming security threats with automatic remediation, sandboxing, anti-virus, intrusion prevention, and content filtering. The castle wall deters and catches threats.

Gatehouse = Multifactor Authentication. MFA provides an additional layer of security by verifying your identity using more than one method. For example, MFA prevents unwanted access to critical information by verifying usernames and passwords with an additional secret code, usually delivered through a mobile device or notification. The Gatehouse provides an extra layer of security when accessing assets (like files or software programs) that are on your network or in the cloud.

Guards = Anti-Virus. Anti-virus keeps your business safe from known cybersecurity threats and bad actors. The guards need to be informed or see something illegal happening before responding.

Masons = Patching. Maintains your hardware, software, operating system, and security with regular code updates as new threats and vulnerabilities are detected. Patching works like masons who identify and repair cracks, holes, and other weak points in the castle's walls.

Guardian = EDR. Endpoint Detection and Response (EDR) monitors your entire business for suspicious behavior in real-time to detect cyberattacks, isolate infected machines, alert administrators, and remove cyberthreats. Like an omniscient guardian, EDR recognizes advanced, sneaky attacks and shuts them down before they attack your business, anywhere an asset is located.

Library = User Education. Teaches users about safe IT practices, such as internet, email, and peripheral device usage; password management; and data control. User educations also includes testing to ensure students retain what they have learned.

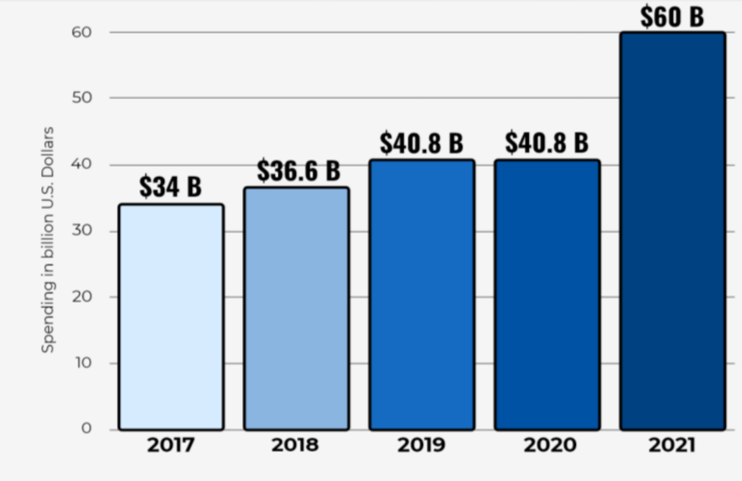
Clerks = Security Information and Event Management (SIEM). Records and stores your system's log files for use if a cyberattack occurs. Think of SIM like clerks recording a history of the castle's happenings for future scholars to reference.

Royal Archives = Data Backup. Whether you're on-premise or working from home, company files are stored, up-to-date, and protected.

Moat = Email Security. Automatically scans email for spam, unlawful interception, phishing, malicious attachments. Encrypts outbound emails containing sensitive data and employs advanced threat protection (ATP) to identify bad actors based on their behavior. The moat ensures only safe traffic enters and exits the castle.

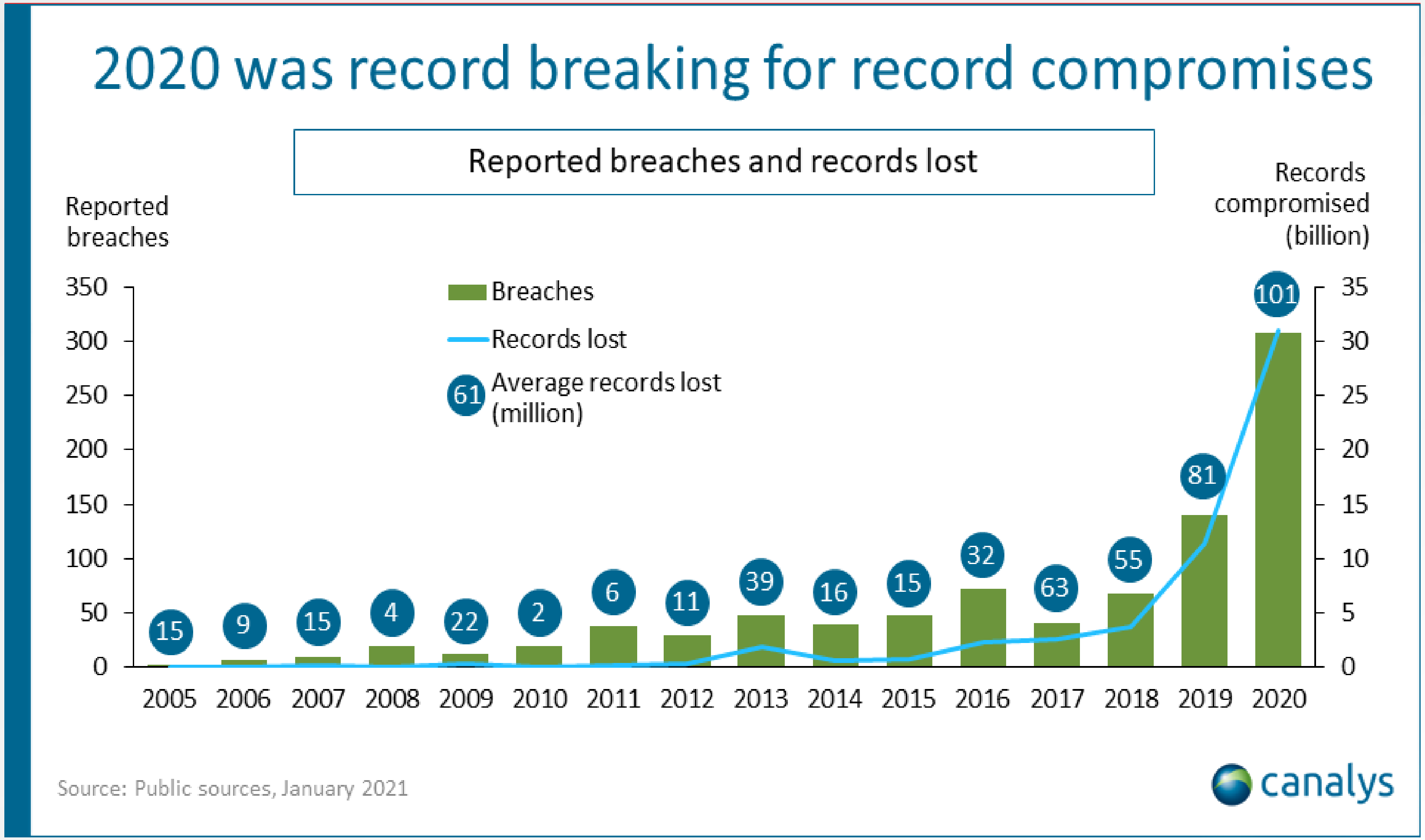
Do we need more evidence that legacy approaches to cybersecurity are broken?

Despite significant increases in cybersecurity spend the number of cybersecurity incidents continues to increase



There are 2 types of organisation:

- Those who have **experienced and reported** a cybersecurity breach (**cyber aware**)
- Those who are **yet to identify and report** that they have had a cybersecurity breach (**cyber unaware**)

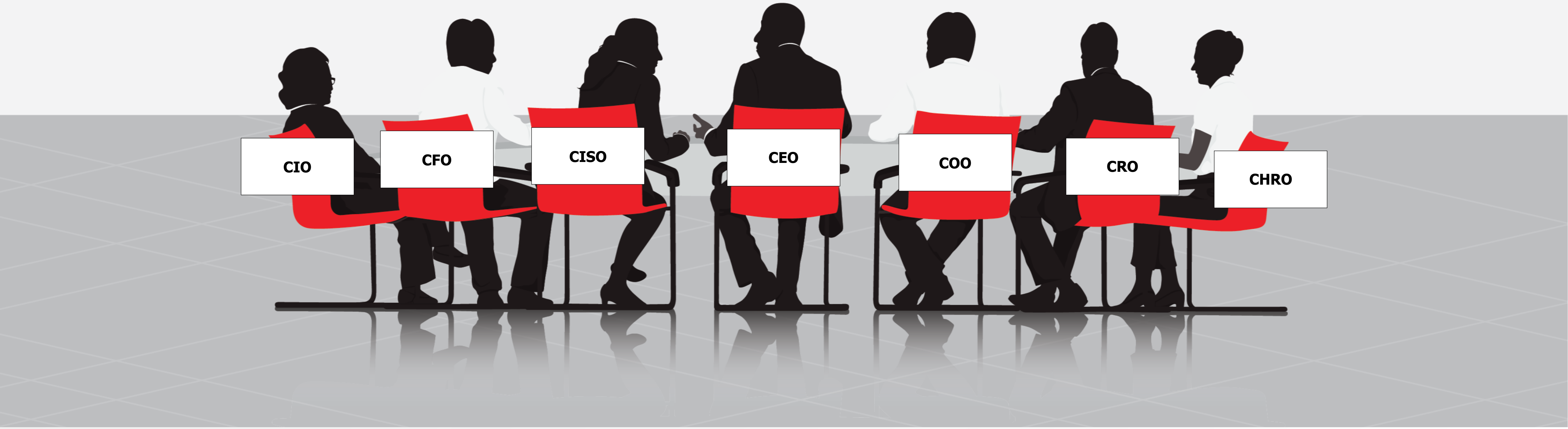


2020 was record breaking for record compromises

Source: Public sources, January 2021

As a consequence the conversation is changing at the C-Suite Level

Technology risk related budgets are controlled at C-suite most (80%-100%) respondents: primarily the CIO/CTO (50%), followed by COO, CFO and CRO



Digital Trust is changing the conversation at the C-Suite level

>80%

of businesses increased budget by more than **25%** in past three years

76%

of organizations view **digital risk as a business challenge,** and not a tech issue

64%

of organizations **lack trust in AI** yet view as a strategic business priority

73%

organizations view **Digital Supply Chain** risk as a critical business risk

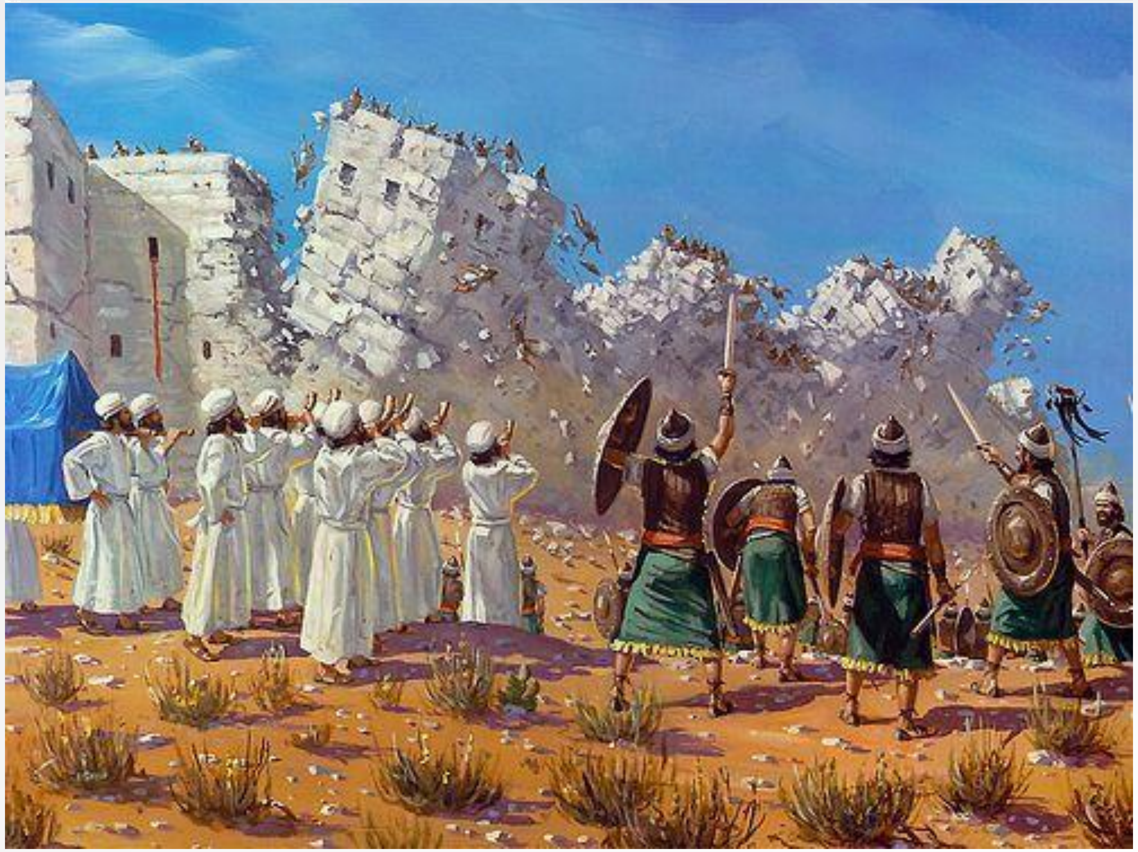
Looking Back to the Future

In late 2003, the Jericho Forum recognised that a new approach to Cybersecurity was required

20 years ago, it was referred to as **DEPERIMETERISATION** - today we call it **ZERO TRUST**, but the overall principles of those soothsayers remains the same

Reliance on layers and layers of technology based perimeter based defence designed to prevent doesn’t work

Monitoring and detective controls need to be pragmatically balanced with preventative solutions



Navigating towards Digital Trust

Introducing Digital Trust

Trust in the digital interactions and relationships between business, people and things

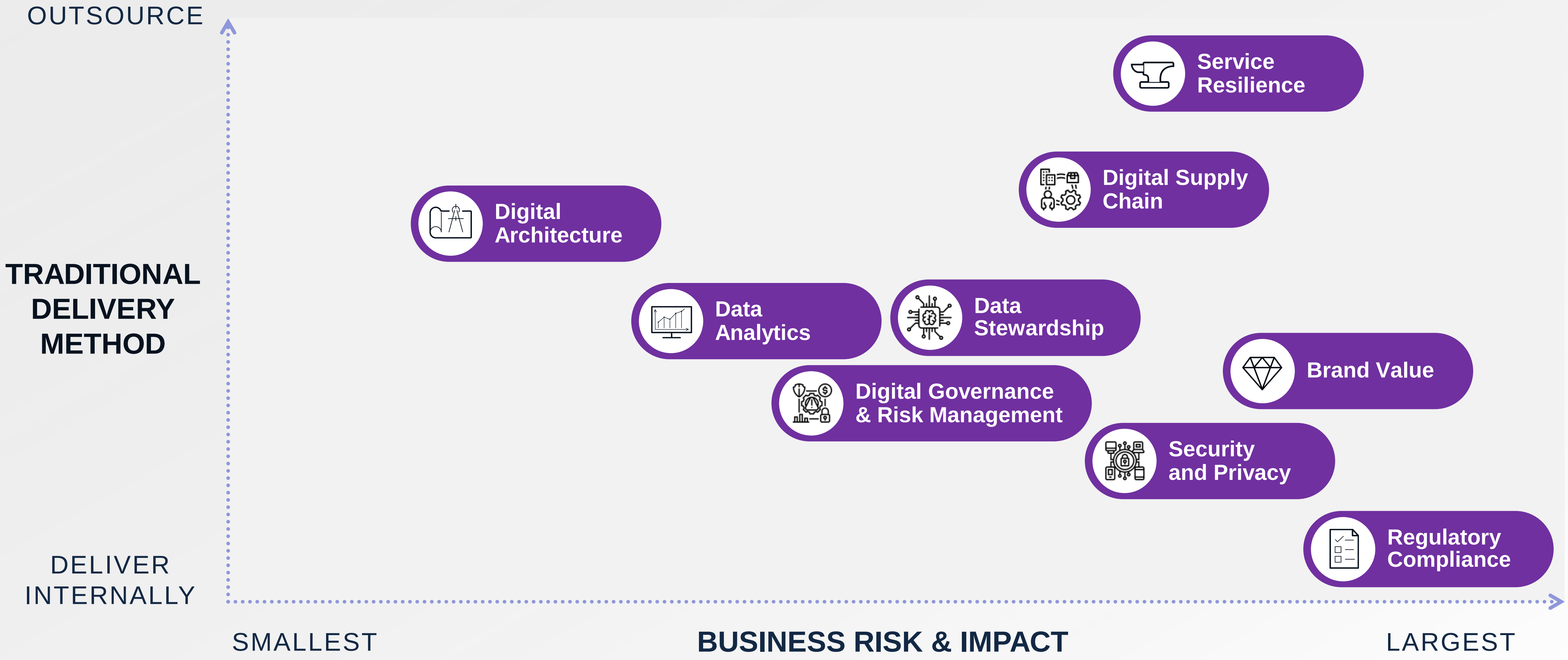
Why now?

- COVID acceleration
- Loss of faith that traditional investments in cybersecurity will prevent breaches
- Businesses want/need confidence (independent assurance) in large digital investments

What's needed?

- Business relevant response
- Proactive risk management focus on monitor, detect and respond
- Heightened awareness across cybersecurity industry that the solution lies within people, process and technology as well as effective and sustained governance

What are the greatest areas of cyber resilience risk and how are they managed?



The societal need for Digital Trust

GOVERNMENT
MANUFACTURING
HEALTHCARE
TRANSPORT & MOBILITY
Digital Trust… bringing order to digital chaos
ICT
BUILT ENVIRONMENT
FOOD & RETAIL
ENERGY
CO2

bsi.

Q&A

bsi.