Digital trust

Building trust is a journey worth taking
Top Breaches of 2018

Aadhaar 1.1 billion

Marriott Starwood Hotel 500 million

MyFitnessPal 150 million

Quora 100 million

Cambridge Analytica 87 million

Google + 52.5 million
Information Security in Organizations

Silo InfoSec risk mitigations

Integrated InfoSec programs

Mature programs to respond to hidden digital risks
The PUSH

New Regulations
• GDPR
• New NAFTA
• California Consumer Privacy Act

Updated Frameworks
• NIST CSF 1.0 -> 1.1
• CIS CSC Framework v6.0 -> v7.0
Global State of Information Security® Survey (GSISS) 2018

9500 business leaders across 122 countries participated in 2018
40% respondents feel a successful cyber attack can cause loss in operations.

And yet … *Less than half of survey respondents have adopted many of the key processes for uncovering cyber risk in business*

- Active monitoring/analysis of information security intelligence: 48%
- Vulnerability assessments: 45%
- Threat assessments: 45%
- Penetration tests: 42%
How prepared is your workforce?

34% of respondents say their company has an employee security awareness training program.

Employees are responsible for 27% of all cyber security incidents.

Source: GSISS
Does your business include cyber and privacy management in their digital transformation?
Board is provided with adequate reporting on metrics for cyber and privacy risk management?

Source: GSISS
“High preparedness does not necessarily mean low risk.”

USA is most prepared and committed to cyber security amongst all member states
~ The UN’s 2017 Global Cybersecurity Index

The No. 1 business risk in US: “large-scale cyberattacks or malware causing large economic damages, geopolitical tensions, or widespread loss of trust in the internet.”
~ World Economic Forum