Cyber Security Case Study

IMPROVING CYBER SECURITY

Linking Risk, Culture & Performance

$1T
Ransomware payments first 6 months of 2021

$132 B
Global spend on cyber security in 2020

600%
Increase in cybercrime in 2020

90%
Breaches from human mistakes and errors

BACKGROUND

Cybercrime involves the damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, reputational harm, damage to critical infrastructure and in some cases, loss of life. And its big business, with ransomware payments for the first 6 months of 2021 reaching $1 trillion.

Traditionally, cyber security has been a technology issue, resulting in a large increase in IT budgets. In 2020 the world spent $132 billion on cyber security technology and services. However, the global cost of cybercrime in 2020 was nearly $6 trillion. Obviously, our reliance on technology for cyber security is not working.

CYBER SECURITY AS A BUSINESS ASSET

We view cyber security as an enterprise business issue and as such everyone in the organization needs to be accountable, not just the CISO. By viewing cyber security as a business asset, organizations can significantly strengthen their cyber posture, reduce risk, and create added enterprise value.

Top 10 Cyberattacks by Industry:

1. Finance & Insurance
2. Manufacturing
3. Energy & Utilities
4. Retail
5. Professional Services
6. Government
7. Healthcare
8. Media
9. Transportation & Logistics
10. Education

"Cyber threats are a mirror the entire organization, not just the cyber security function."

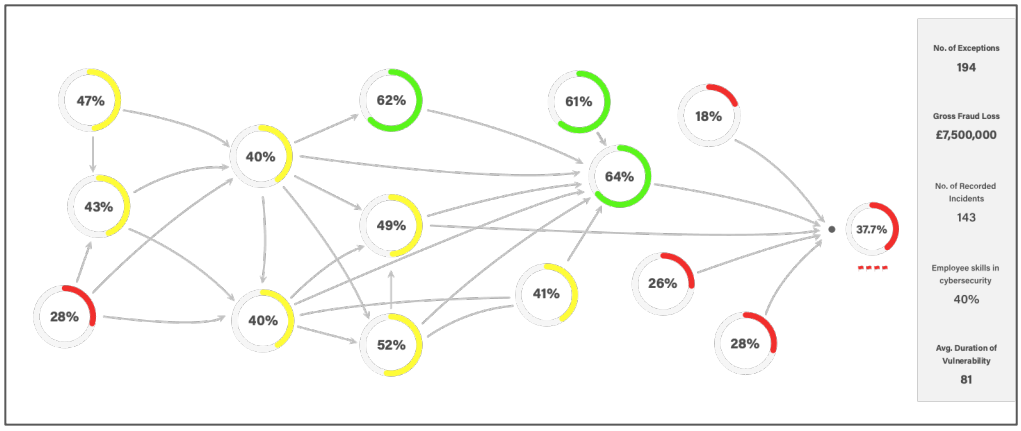
~Christiane Wuillamie OBE

Business Benefits of a strong cyber security culture:

- Reduced Probability of Business Disruption & Faster Recovery
- Reduced fines associated with data loss
- Increased Customer Loyalty and Repeat
- Business Greater Market Reputation and
- Business Valuation: Greater Productivity
- Employee Retention

BUILDING A STRONG CYBER SECURITY CULTURE

Identifying Systemic Cyber Risk:
To understand the impact of cyber risk, a customized systemic cyber security ecosystem map helps CISOs engage all functions in stepping up to their cyber accountability. Using this map, senior leaders can open productive conversations inside the organization on cyber risk mitigation, making cyber security everyone's accountability.



Board Commitment:
All board members should have personal cyber security training, so they fully understand their role in overseeing and supporting cybersecurity. A home check of their technology environment should be part of each Board member's education. Also, the Board cannot rely on having one member with cyber expertise as this lets others opt-out of their important risk responsibilities.

Responsible Leadership:
The majority of Business Heads and Functional Leaders believe cyber security is primarily a technology issue. The CISO must proactively engage with business leaders and functional heads to help them understand how cyber threats increase business risks. The CISO should also help promote greater collaboration and information sharing between business lines and functions, with a set of shared objectives around enterprise cyber security.

Poor Cyber Security is a Business Cost

$3.8 million:
Avg. cost of cyber breach

280 days:
Avg. time to identify and contain a breach

2 – 4 weeks:
Avg. time to recover from a cyber breach

Customer Trust:
A cyber-attack damages customer trust and reduces loyalty, resulting in loss of revenue.

Downtime:
A ransomware attack shut down Colonial Pipeline for 6 days, impacting several million customers and closing gas stations in 6 states.

"Every function must become cyber-responsible. To blunt cybercrime, we must adopt a culture of rigorous cyber hygiene."

~Rick McElroy
Cyber Security Strategist
VMware

Since organizations are shadows of their leaders, it is imperative that the senior leaders not only actively support the cyber security function but also be visible with this support. Townhall meetings, as well as internal communication, should stress the importance of cyber security and everyone's accountability in creating a cyber-safe organization.

Risk Management:
Regular tabletop exercises for the Board, executives, and managers are important to build rapid response and recovery for a cyber incident. It is up to the CISO and the cyber team to create and facilitate these important cyber security exercises, and to ensure they are mandatory on a regular basis.

Design for Security:
When products connect to the internet and company networks, they dramatically increase vulnerability. Design for Security must become standard practice for **EVERY** new digitally enabled product and service.

Internal Communications:
In many organizations, poor cross-functional communications and lack of cooperation create unnecessary cyber vulnerabilities and slow recovery efforts. The CISO needs to support the internal communications function to develop timely cyber security communications, including news about recent incidents.

Secure Your Supply Chain:
Many successful cyber breaches and ransom attacks enter a company through supply chain partners. In most cases, these relationships are overseen by IT, legal and logistics, but must include the cyber security function. The CISO needs to work closely to help the enterprise secure its supply chain partners since the CISO is responsible for cyber risk.

Employee Care and Training:
During the global COVID pandemic, working from home and hybrid working schedules have dramatically increased the cyber attack surface since many home environments are not secure. The CISO needs to lead the company in policies, practices, and training to make certain that everyone, from the Board to the new joiner has their personal home environments fully secured.

Link Cyber Security to Business Priorities:
The CISO must understand the company's business priorities, how they are impacted by cyber security and develop his cyber strategy in conjunction with business priorities.

"All board members need to fully understand the role they play in overseeing cybersecurity."
~IT Pro magazine, 2021

Building a Strong Cyber Security Culture

- Identify systemic cyber risks
- Board Commitment
- Engaging Business Leaders
- Risk Management Design for Security Internal
- Communications
- Secure Supply Chain
- Employee Care and Training
- Link Cyber Security to Business Priorities
- Industry Collaboration and Information Sharing

"PYXIS identifies the hidden cyber risks in culture, processes and technology."

~Head of Cyber Strategy, Global FMCG Company

Industry Collaboration and Information Sharing:
All industries are facing similar cyberattacks. Since cybercriminals share vulnerability information among themselves, it is time for strong cyber security collaboration and information sharing among organizations. The CISO is perfectly positioned to help build collaboration and cyber information sharing. Recently the insurance industry came together to build a database and collaboration platform for sharing insurance-related cyber security data and knowledge.

"PYXIS Culture Technologies has comprehensive experience and a unique methodology to improve cyber security culture."
~Stéphane Nappo
Cyber Security Expert
& Global CISO

PYXIS:
YOUR BUSINESS PARTNER FOR CYBER SECURITY

We differ from traditional consulting firms in two important areas. We combine over 40 years of experience in how culture impacts performance with deep operational experience in technology management, digital transformation, cyber security, and business turnarounds.

At PYXIS Culture Technologies we have pioneered an ecosystem modelling approach for understanding, measuring, and managing cyber security risks to improve business performance. Using systems analytics and proprietary algorithms along with internal company data, we can identify and map the causal factors inside your organization that have a significant impact on cyber security and business performance.

SUMMARY

- Cyber security is a business issue, not a technology issue.
- The CISO needs to help build an enterprise approach to cyber security
- The Board and Senior Leaders must have a shared cyber security agenda
- Sharing information about recent incidents helps all employees learn and become more accountable
- The cyber strategy needs to support the business strategy.
- Proactive management of Third-Party cyber risks is critical to good cyber security

For more information about an enterprise approach to cyber security, contact

Christiane Wuillamie OBE cw@pyxisculture.com
Visit our website: www.pyxisculture.com