Cyber Security Case Study

IMPROVING CYBER SECURITY

In a Multinational Consumer Goods Company

$ 3.8M
Average cost of cyber Breach per company

267 days
Average time to Detect a breach

600%
Increase in cybercrime in 2020

90%
Breaches from human mistakes and errors

A CYBER SECURITY DILEMMA

The Head of Cyber Security Strategy for a $55 billion multinational consumer goods company with a strong sales and cost-control culture was concerned about the growing wave of global cybercrime. She wanted to better understand and identify the hidden cultural and organizational levers for improving cyber security. However, in this organization cyber security was seen as a technology issue, not a business issue, and the cyber budget was incorporated into the Information Technology department.

In 2020 the world spent $132 billion on cyber security technology and services. However, the global loss to cybercrime in 2020 was nearly $6 trillion. Obviously, reliance on technology alone for cyber security is not working. And the majority of successful cyberattacks are the result of human mistakes and errors.

CYBER SECURITY AS A BUSINESS ISSUE

The Head of Strategy was convinced that every part of the company had an important role to play in cyber security. Efforts to engage with other functions, such as Finance, Risk, HR, Internal and External Communications, and Business lines gained little support. In working with PYXIS Culture Technologies, she was able to reframe cyber security as a business and cultural issue that got the attention of senior leadership.

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:

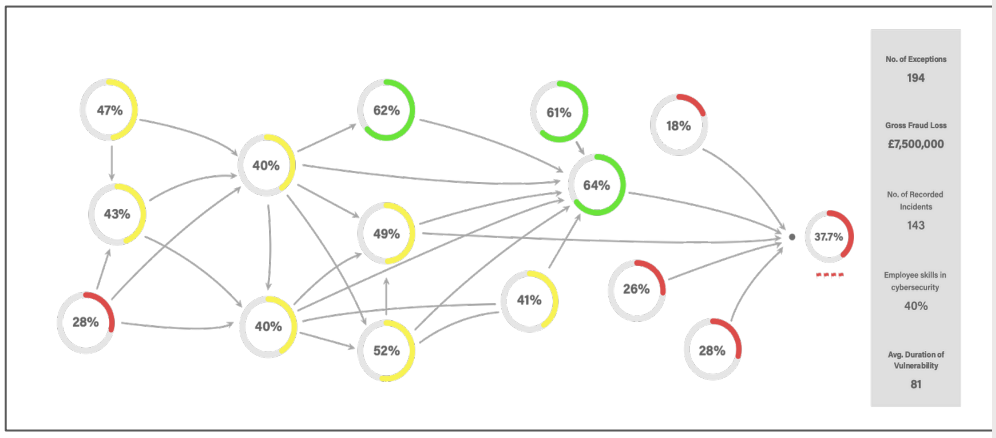
- Reduced Probability of Business Disruption & Faster Recovery
- Reduced fines associated with data loss
- Increased Customer Loyalty and Repeat
- Business Greater Market Reputation and
- Business Valuation: Greater Productivity
- Employee Retention

IDENTIFYING & MITIGATING CYBER SECURITY RISKS

Intent on building a strong cyber security culture across their multinational footprint, PYXIS helped to build a roadmap for a strong cyber security culture.

Map Cyber Security Causal Factors:
After conducting over 50 interviews with company cyber security experts and business managers across 18 countries, PYXIS and key cyber security employees identified multiple causal factors within the organization that impact cyber security.

Using the data gathered, the PYXIS platform and algorithm created a visual map of the cyber security causal factors, with numerical and colour coded scores, as well as an overall cyber security effectiveness score. In addition, historical and current business metrics were linked to the culture map.



Beyond the usual factors such as training and phishing email exercises, the team uncovered many previously unidentified causal factors. These included complicated internal IT and cyber security policies, cumbersome work processes, supervisor demands for cost control, peer pressure not to speak up about mistakes, weak third-party cyber practices, poor oversight of Access Management, lax physical security, and lack of support from senior leadership and the Board. The team also highlighted the importance of cyber-safe home working and family cyber awareness as critical cyber safety issues.

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

Identify Systemic Cyber Risks:
Quantitative and qualitative data and information for the PYXIS cyber mapping algorithm was gathered from internal company data, including historical cyber metrics and past employee engagement surveys. In addition, a custom cyber security culture assessment was developed and sent to cyber security employees, managers and supervisors.

Scenario Planning & Best Practice Improvements:
The PYXIS platform contains a library of best practices specific for each causal factor. The internal cyber team added additional best practices specific for their international locations and requirements. A scenario planning function built into the PYXIS platform allowed us to model which best practice initiatives delivered strong cyber security improvements, as well as Return on Investment.

The team selected three cyber improvement initiatives to focus on. These improvement initiatives were, greater engagement with business leadership, more oversight of Third-Party suppliers and supply chain contractors, and stronger oversight of Access Management.

Track Cyber Safety & Business Metrics:
The PYXIS platform and methodology also links the cyber security culture to important business metrics, which can then be tracked on a regular basis. This capability allows the cyber security team to constantly assess and adjust their internal practices to improve performance.

Engage the Board & Senior Business Leaders:
With the visual cyber security maps, the cyber security team now has the capability to communicate with the Board and Senior Business leaders how cyber security is an enterprise issue, and not just a technology issue.

Rather than wading through the traditional thick cyber security quarterly reports, the visual map makes it easy to spot cyber vulnerabilities and helps the Board and senior leader open effective discussions about how to better protect the company and its customers. With this new approach to cyber security culture, the cyber security function moves from a cost centre to an effective business partner.

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.

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

Identifying & Mitigating Cyber Security Risks

- Map Cyber Security Causal Factors
- Identify systemic cyber risks
- Scenario Planning & Best Practice Improvements
- Track Cyber Safety & Business Metrics:
- Engage Board & Senior Business Leaders
- Industry Collaboration and Information Sharing

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

~Head of Cyber Strategy, Global FMCG Company

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.
- Industry collaboration and threat information sharing is critical to building a strong cyber security culture.

"PYXIS Culture Technologies has comprehensive experience and a unique methodology to improve cyber security culture."

~Stéphane Nappo
Cyber Security Expert
& Global CISO

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

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