pyxis

Cyber Security Case Study

REDUCING CYBER SECURITY RISKS
A Retail Banking Case Study

$ 3.8M	267 Days	600%	90%
Average cost of cyber breach per company	Average time to detect a breach	Increase in cybercrime in 2020	Breaches from human mistakes and errors

THE CISO'S DILEMMA

The Chief Information Security Officer (CISO) of an International Retail Bank needed a powerful way to help senior business leaders and the Board understand the importance of cyber security, and the bank's increasing vulnerability to cybercrime. Traditional cyber briefing documents were too detailed and filled with technical jargon. In addition, most Board members and senior business leaders believed that cyber security was a technology issue, and the cyber budget was incorporated into the Technology budget.

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 was not working. And the financial services industry was under constant cyber-attack from criminal gangs and Nation State actors.

CYBER SECURITY AS AN ENTERPRISE ISSUE

The CISO was convinced that every part of the bank had an important role to play in building a strong and safe cyber security culture. Although he made every effort to engage with other functions, such as Finance, HR, Internal and External Communications, and Business lines, he gained little support from other areas. Working with PYXIS Culture Technologies, the CISO began to reframe cyber security as a business issue.

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 within the bank, the CISO and his cyber leadership team followed a proven methodology developed by PYXIS Culture Technologies.

Map Cyber Security Causal Factors:
In a three-hour workshop the cyber security leadership team worked together to identify the many causal factors within the organization that have an impact on employee actions concerning cyber security. Beyond the usual factors such as training and phishing email exercises, the team was guided by PYXIS to uncover the many hidden causal factors driving cyber security.

These hidden causal factors include complex 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, lack of connection between physical security, IT and Cyber 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; and this was before the Pandemic!

Identify Systemic Cyber Risks:
To gather quantitative and qualitative data and information for the PYXIS cyber mapping algorithm, the team spent a week gathering internal company data from a variety of functions, including historical cyber metrics and past employee engagement surveys. In addition, a custom cyber security culture assessment was developed and sent to all managers and supervisors.

Using the data gathered, the PYXIS algorithm developed numerical and colour coded scores for each causal factor, as well as an overall cyber security effectiveness score. Also, historical and current business metrics were linked to the culture map.

Poor Cyber Security is a Business Cost

$3.8 million:
Avg. cost of cyber breach

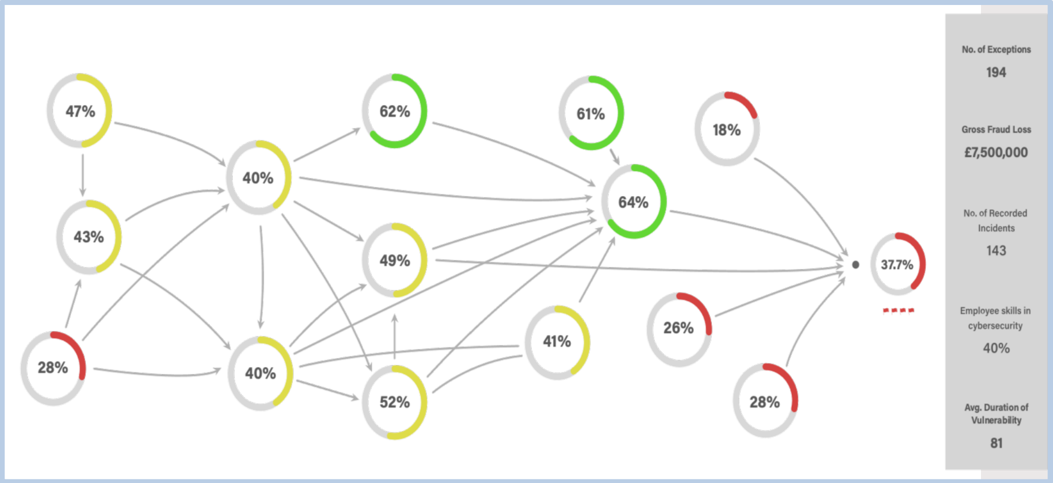
267 days:
Avg. time to identify and contain a breach

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:
The cost of company downtime due to a successful cyberattack is 5 times the cost of a ransom payment

> "Every function must become cyber-responsible. To blunt cybercrime, we must adopt a culture of rigorous cyber hygiene."
>
> ~Rick McElroy
> Cyber Security Strategist
> VMware



Scenario Planning & Best Practice Improvements:
The PYXIS platform contains a library of best practices specific for each causal factor. The bank cyber team added additional best practices specific for their international locations and requirements. These best practices were then used with a scenario planning function built into the PYXIS platform that allowed the team to model which best practice initiatives delivered the best cyber security improvements, as well as calculating Return on Investment (ROI) for each initiative.

The team selected several cyber improvement initiatives to focus on in the coming months to improve their overall cyber security culture and cyber safety. These improvement initiatives were, greater engagement with business leadership, more oversight of Third-Party suppliers and contractors, risk management, and data privacy. They also focused on revising several cyber policies and processes for easier compliance.

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 CISO now has the capability to easily 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 the current cyber vulnerabilities and helps the Board and senior leader open effective discussions about how to better protect the bank and its customers.

With this new approach to cyber security culture, the CISO can easily use cyber security to better support business line objectives and strategies. The cyber security function thus moves from a cost centre to an effective business partner.

Map Cyber Security Causal Factors

Identify Systemic Cyber risks

Scenario Planning & Best Practice Improvements

Track Cyber Safety & Business Metrics

Engage the Board & Senior Business Leaders

Building a Strong Cyber Security Culture

- Identify systemic cyber risks
- Board Commitment
- Engaging Business Leaders
- Secure Supply Chain
- Employee Care and Training
- Link Cyber Security to Business Priorities

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.

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

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