Cyber Security Case Study

SUCCESSFUL HOSPITALS BUILD A STRONG CYBER SECURITY CULTURE

$3.5M
Average cost of cyber breach

56 %
Cyberattacks successful

Ransomware
Top cyber threat to healthcare sector

50 X
Hospital downtime costs greater than ransom payment

BACKGROUND

Cybercrime is growing rapidly in the healthcare industry as cyber criminals recognize the weaknesses of legacy systems in most hospital IT functions. In addition, the consequences could be life threatening and most hospital administrators prefer to pay the ransom to avoid potential lethal consequences. Add to this the fact that hospital staff are traditionally stressed and overworked, plus little cyber training is given or encouraged. It's a perfect storm and ripe pickings for cyber criminals.

Recently, a ransomware attack on Scripps Health in San Diego succeeded in stealing 147,000 patient records. The result was over $21 million in data recovery costs, plus several class-action lawsuits. Not to mention the multimillion dollar ransom paid. Around the world cyber attacks on hospitals and the healthcare industry have exploded. Between 2019 and 2020, cyber attacks increased by 470%. In 2020, more than 33% of healthcare organizations reported ransomware threats.

CYBER SECURITY CULTURE IS YOUR BEST FIREWALL

We view cyber security as an organization-wide issue, not just a technology issue. Every employee, Trustee and contract worker needs to be accountable, not just the IT department. By viewing cyber security as an enterprise asset, hospitals can significantly strengthen their cyber posture, reduce risk, and safeguard employee and patient well-being.

Top 10 Hospital Cyber Risks:

- Seen as a technology issue
- Not part of hospital strategy
- Unsafe IoT medical devices
- Legacy systems
- Board doesn't understand cyber risks
- Cyber training not mandatory
- Clicking on Phishing emails
- Doctors demanding special access
- Weak data backup & recovery plan
- Fatigue and stress

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

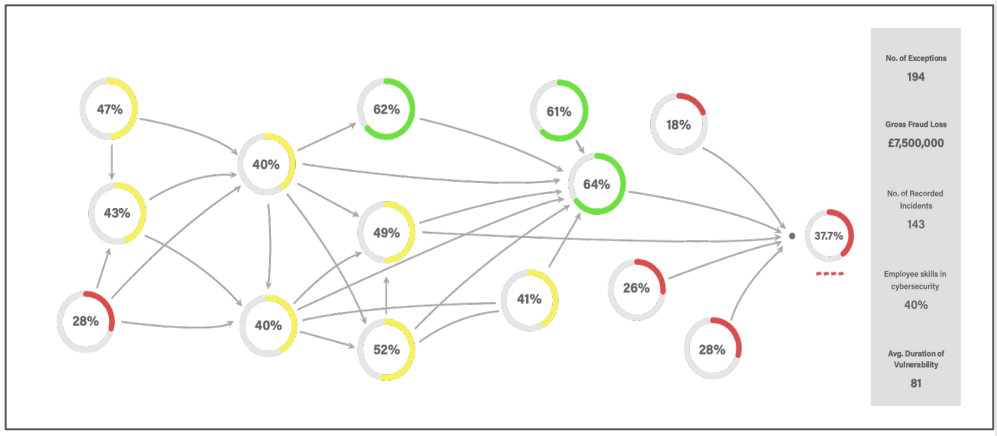
~Christiane Wuillamie OBE

Benefits of a strong cyber security culture:

- Reduced Probability of Disruption
- Faster Recovery
- Reduced Costs Associated With Data Loss
- Increased Public And Patient Trust
- Employee Loyalty And Retention
- Reduced Stress On Staff

BUILDING A STRONG CYBER SECURITY CULTURE

Identifying Systemic Cyber Risk:
To understand how your organizational culture impacts cyber security, it is important to identify the internal drivers of cyber security. A cyber culture map can identify the systemic strengths and risks in your cyber ecosystem. A visual cyber security ecosystem map helps engage all functions in understanding their cyber accountability. Using this map, senior leaders can open productive conversations with all departments on cyber risk mitigation, making cyber security everyone's accountability.



Trustee Understanding and Commitment:
All hospital trustees 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 this education. Also, the Board of Trustees 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 Hospital Administrators believe cyber security is primarily a technology issue. The Head of Technology must proactively engage with administrators and department heads to help them understand how cyber security culture is a key factor in cyber security and how cyber threats increase patient risks. The head of technology should also help promote greater collaboration and information sharing between departments and help develop a set of shared objectives and metrics for cyber security.

Weak Cyber Security is a Significant Risk

$3.5 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

Public Trust:
A cyber-attack damages public and patient trust and reduces employee loyalty

Recovery Costs:
The cost of data recovery after a ransomware attack is 50 times greater than the 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

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

Risk Management:
Regular tabletop exercises for the Trustees, senior hospital executives and department heads are important to build awareness, commitment and rapid response and recovery from a cyber incident. In addition, training should be mandatory for all hospital staff so they can understand and support good cyber hygiene.

Design for Security:
Whenever equipment connects to the internet and the hospital network, it dramatically increases vulnerability to cybercrime. It is up to the hospital technology staff to ensure that all digital equipment has been built using a Design-for-Security approach.

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

Secure Your Supply Chain:
Many successful cyber breaches and ransomware attacks enter a hospital through supply chain partners. In most cases, these relationships are overseen by IT, legal and logistics, but must include the cyber security function. It is imperative to ensure that all supply chain partners implement cyber safe protocols.

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. Every hospital needs to put in place policies, practices, and training to make certain that everyone, from the Board of Trustees to the new joiner has their personal home environments fully secured. Plus, employee training in cyber security awareness needs to be mandated, not optional.

"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

Collaboration and Information Sharing:
All industries are facing cyberattacks. Since cybercriminals share vulnerability information among themselves, it is time for strong cyber security collaboration and information sharing between hospitals. Hospital leadership must build collaboration and cyber information sharing with all hospitals in their area, and beyond. Recently the insurance industry came together to build a database and collaboration platform for sharing insurance-related cyber security data and knowledge. Hospitals can do the same.

"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

PYXIS Culture Technologies, Ltd is 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 hospital needs to help build an enterprise approach to cyber security
- The Board and Hospital Administrators 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 be a part of the hospital strategic plan and vision.
- Proactive management of Third-Party cyber risks is critical to protecting your hospital.
- Information sharing and collaboration with other hospitals is critical in building a strong cyber secure hospital.

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

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