Technology and Cybersecurity Risk Management

BCNPHA - Housing Central Conference - November 19, 2024

Presenter/Moderator – Mike Klein | Vice President, Information Management & Technology, BC Housing

BC HOUSING

HOUSING CENTRAL®

BC's Affordable Housing CONFERENCE

Housing Provider Technology Support

Why Cyber Security Matters For Non-Profit Housing Providers

The Stakes Are High

Sensitive Data at Risk

Tenant information, payment records, and operational systems

Operational Continuity

Disruption of services and harm to vulnerable populations

Reputation and Trust

Undermine confidence from tenants, funders, and partners, even spreading the breach to those stakeholders

Risks for Non-Profits

Data Sensitivity

Handling client and donor information

Budget Constraints

Limited resources for cybersecurity measures

Human Factor Vulnerabilities

Social engineering, phishing, weak passwords, trust

Third-Party Risks

Dependence on external vendors and partners

Why Risk Management is Important

Growing dependence on digital tools for service delivery and fundraising

Sensitivity of data continues to compound with new clients and more information

Non-profits are frequent targets due to limited cybersecurity resources, and hackers know this

Understanding Technology & Cybersecurity Risks

Phishing and Social Engineering	**Employees targeted with deceptive emails or messages**
Example: ***Fake invoice emails trick staff into transferring funds***	

Human Error	**Misconfigurations or accidental data exposure by staff**
Example: ***Security protections being misconfigured; lost unencrypted USB stick***	

Ransomware	**Data encrypted, with attackers demanding ransom for restoration**
Example: ***Organization unable to access tenant records for weeks***	

Supply Chain Vulnerabilities	**Risks from third-party vendors' cybersecurity vulnerabilities**
Example: ***Third Party is hacked with data exposure of sensitive data that has been shared***	

The Role Of the Board and Senior Management

Why Leadership Support Matters:

- **Cybersecurity requires investment in tools, processes, and training.**
- **Leadership sets the tone for a culture of security and accountability.**
- **Visible commitment builds trust among donors, staff, and clients.**

Responsibilities of the Board and Executives:

- **Prioritize cybersecurity as a governance issue.**
- **Allocate adequate resources for cybersecurity initiatives.**
- **Regularly review and approve cybersecurity policies and budgets.**

Actionable Steps:

- **Include cybersecurity as a standing agenda item in board meetings.**
- **Assign a board member or executive as a cybersecurity champion.**
- **Conduct periodic briefings and training sessions for leadership.**

Key Pillars of a Good Cybersecurity Program

Risk Assessment

Identifying and prioritizing vulnerabilities

Mitigation Strategies

Implementing robust preventive measures

Governance

Establishing clear policies and accountability

Continuous Improvement

Regularly updating and monitoring systems

Building Resilience Through Risk Assessment

How to Assess Cybersecurity Risks

Identify Key Assets

Examples: Tenant database, financial systems, and communication tools

Evaluate Threats and Vulnerabilities

Analyze how attackers could exploit systems or processes

Output:

Risk matrix with high, medium, and low-priority items.

Prioritize Based on Impact

Examples: Unprotected tenant data; email system compromise

Document and Review

Maintain an updated risk register with mitigation plans

Mitigation Strategies for Cybersecurity Risks

Layered Defense Approach

Technical Controls

Multi-Factor Authentication (MFA)

Regular updates and patches for all software

Endpoint detection and response tools

Administrative Controls

Written policies for staff and vendors

Periodic cybersecurity awareness training

Physical Security

Controlled access to server rooms or sensitive documents

Cyber Security Governance

Treat cyber security as a strategic priority

- **Securing commitment from the Board and Executive leadership to prioritize cybersecurity**
- **Establish leadership updates and reporting on cybersecurity risks**
- **Establish a Cybersecurity Committee that is assigned responsibility to oversee cybersecurity strategy and initiatives)**
- **Implement a policy framework that develops and regularly updates cybersecurity policies**
- **Allocate a budget for security infrastructure, education and regular assessments/audits**
- **Fostering a Cyber-Aware Culture**

Metrics for Continuous Improvement

Understand Leadership Needs → **Identify Key Areas** → **Develop Meaningful Metrics**

Metric	Value	Trend	Threshold
Critical Vulnerabilities	5	↓ (from 8)	< 3
Mean Time to Detect (MTTD)	2 hours	→ (steady)	< 4 hours
Training Completion Rate	95%	↑ (from 90%)	> 90%
Phishing Test Failure Rate	12%	↓ (from 18%)	< 10%

↓

Taylor Reporting for Leadership → **Establish Reporting Cadence** → **Enable Continuous Improvement**

Incident Response Plans – Preparation is Key

Why does an Incident Response Plan matter?

Swift, coordinated responses minimize damage and restore operations faster

Key Components to consider when building an Incident Response Plan

Preparation	Detection and Identification	Containment	Eradication	Recovery	Communication	Post-Incident Analysis	Legal and Regulatory Compliance
Ensures the organization is ready to respond effectively to incidents, minimizing disruption and protecting critical assets.	Early detection limits damage and reduces response time.	Prevents the incident from spreading and impacting more systems, data, or operations.	Removes the threat and ensures the organization is no longer vulnerable to the same attack.	Restores normal operations as quickly and safely as possible while maintaining stakeholder confidence.	Builds trust with stakeholders, manages reputational risk, and ensures compliance with reporting obligations	Turns an incident into a learning opportunity, improving resilience for the future.	Protects the organization from legal penalties and aligns with industry or regulatory obligations.

Security by Design – Proactive Resilience

Embedding security considerations into the development, implementation, and management of systems and processes from the outset, rather than addressing them reactively

Benefits of Security by Design

Fewer Vulnerabilities: Prevent flaws early, reducing costs later.

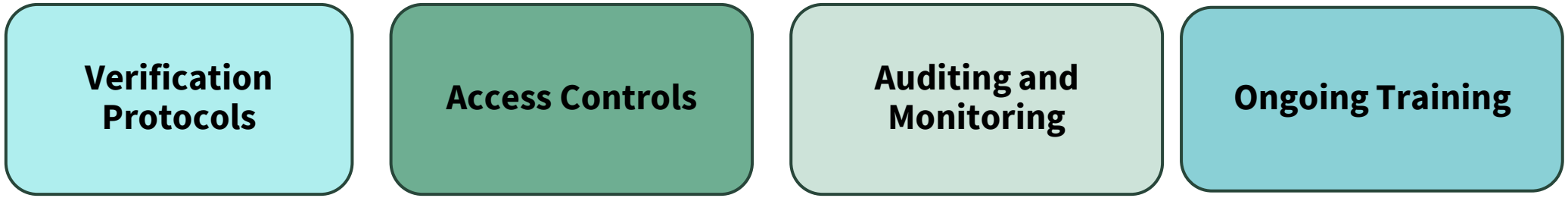
Improved Compliance: Meet regulatory and legal standards.

Increased Resilience: Future-proof systems against evolving threats.

Scenario: A housing organization launches a digital tenant portal for rent payments, maintenance requests, and personal document submissions.	**Security by Design Example**: •During development, the portal integrates **end-to-end encryption** for all tenant data, ensuring it is secure both in transit and at rest. •The system enforces **multi-factor authentication (MFA)** for login to protect accounts against unauthorized access. •Role-based access ensures that staff can only view tenant information necessary for their roles.	**Impact**: Protects sensitive tenant data from breaches, builds trust, and aligns with data privacy laws (PIPA/FIPPA)

Process & Policy Matter - Catching Social Engineering Failures

When Technology Fails, Processes Save the Day



Double-check financial requests through a second channel

Restrict sensitive system access to only authorized personnel

Regularly review system logs for unusual activities

Focus on recognizing phishing and social engineering attempts

Call to Action

- **Conduct a Risk Assessment, identifying your organization's most critical security risks. Elevate high priority risks to the enterprise risk register**
- **Develop an Incident Response Plan or refine existing**
- **Commit to Regular Training and Exercises: Build organizational awareness and readiness**
- **Implement Security by Design Practices, systems and processes**
- **Policies and processes to protect from technology failures**