What Nonprofit Board Members Need to Know About Cybersecurity

Our Presenters

Sandy Ross, CPA, CFE, MSNM
Partner & Nonprofit Practice
Leader, KLR

"when people support each other, incredible things happen."

Jay Longley
Senior Consultant, Envision
Technology Advisors

"Security isn't something you buy, it's something you do"

Agenda Overview

"It takes 20 years to build a reputation but in a few minutes a cyber incident can ruin it."
- **Stephane Nappo**

1. Cybersecurity – What is It?
2. Most Common Threats
3. Impact on Nonprofits
4. Legal and Regulatory Requirements
   - Board Responsibilities and Risk
   - Grant Opportunities
5. Key Takeaways - How to Stay Safe
6. Q&A & What We're Hearing

KLR

What is Cybersecurity?

The practice of protecting computer systems, networks, data, and digital information from theft, damage, unauthorized access, or any other form of cyber threat. It encompasses a range of technologies, processes, and practices designed to safeguard digital assets and maintain information, confidentiality, integrity, and availability.

KLR

What Are the Most Common Cyber Risk Areas?

- Phishing (resumes)
- Personal Risk - Board Members
- Insider Threats

KLR

Q: What resources are available to keep up with the changing landscape of regulations and cyber security?

Impact on Nonprofits

Impact of an Attack on Nonprofits

- Loss of Revenue
- Brand / Reputational Damage
- Loss of Funding
- Employee Layoffs
- Business Closure
- Lawsuits
- Fines
- Personal Liability
- Double Extortion from Threat Actors
- OFAC Sanctions & Funding Terrorism

KLR

Q: When thinking about safeguarding my nonprofit and staff from cybersecurity threats, what are some quick tips or low hanging fruit that we can tackle to minimize risks?

Impact of An Attack on Nonprofits: Prevention Tips

- Use a board platform like Onboard vs. using your personal email for board communication which could include sensitive information

- Read your documentation before you publish

- Board members should have the ability for expert help

- Address known risks

Legal & Regulatory Requirements

KLR

Legal and Regulatory Requirements

- Written Information Security Plan that is executed, tested, and monitored. Updated date and reviewed.
- Organization's compliance obligations
- Current and Former Board Members
- Employees and Former Employees
- Volunteers
- Vendors
- Customers
- Donors

KLR

Q: How do I (as a board member) best protect myself when we're required to give personal and sensitive information to outside parties?

What Every Person Should Know Before Joining A Board...

1. What compliance obligations does the organization have (HIPAA/PCI/201 CMR 17)?
2. How does the organization prove that it is in compliance?
3. When was our most recent penetration test and what were the results?
4. What is the plan to address the findings from the penetration test?
5. Are there any other technology or cyber risks to the organization, and how is the organization addressing them?
6. Does your Board have use of a governance platform such as OnBoard or BoardEffect?
7. Does the organization have the ability to track and revoke access to ALL data, regardless of location (USB / Personal Email / Home Computer / Dark Web)?
8. Does the board have access to the organization's CCO/CSO/CISO to answer any questions and ensure organizational risk is brought to a minimum?

KLR

Q: What kinds of insurance coverage should organizations have?

Q: Where can I learn more about opportunities to apply for technology grants?

KLR

Key Takeaways to Stay Safe

KLR

Q: Biggest cyber concerns going forward and thoughts on "bad guys" using AI

Key Takeaways

1. Know the organization's compliance obligations, and the associated regulations.
2. Understand the laws that you, and the organization, are subject to
3. Review where the organization falls short so that the deficits can be understood and mitigated.
4. Have an open dialog with the stakeholder who is responsible for the organization's cybersecurity.
5. Ensure that your organization performs vulnerability testing, and cybersecurity assessments at least annually.
6. Review the kinds of data your business collects, where it is stored, how it is classified, if it has compliance obligations, and how the organization meets those requirements.
7. Ensure that the organization has a WISP or equivalent, and that the items contained within are being followed.
8. Review the organization's policies (Data Privacy, Mobile Device, etc.) and audit if the policies are being enforced.
9. Review the insurance policies, and ensure the organization is meeting the requirements set forth within the policy.
10. Allocate a portion of the overall budget for cybersecurity, and review to ensure the funding is adequate.

AT A GLANCE

280+ Total Personnel
45 Partners

Offices in Boston, Geneva, Lausanne, Newport, Pawtucket, Providence, Shanghai, & Waltham

Member of the Leading Edge Alliance, a global association of CPA firms

KLR Affiliates

KLR Executive Search Group, LLC

KLR Wealth Management, LLC

KLR Outsourcing, LLC

Envision Technology Advisors, LLC

Our Services

Audit & Accounting	International Tax Services
Business Valuation & Litigation Support	Insurance Services
Cost Segregation Studies	Investment Services
Cyber Security Services	Mergers & Acquisitions
Digital Transformation	Outsourcing
Executive Search	Research & Development
Financial & Estate Planning	State & Local Tax (SALT)
Financial & Tax Due Diligence	Strategic Planning
Information Security Services	Technology Consulting

We're Here to Help

Sandy Ross, CPA, Partner

Nonprofit Practice Leader, KLR

sross@kahnlitwin.com

Jay Longley, Senior Consultant

Envision Technology Advisors

Jay.Longley@envisionsuccess.net

BECOME FUTURE READY.

KLR Executive Search Group, LLC

KLR Outsourcing

KLR Wealth Management, LLC

Envision Technology Advisors, LLC

KLR