Nonprofit
Risk Management
Center

VOL. 29 • NO. 3 • FALL 2020

# Risk Management ESSENTIALS

Tips, Knowledge and Tools for Nonprofit Organizations

THE CYBER RISK ISSUE

## Demystifying Cyber Liability Insurance

*By Whitney Thomey*

Every nonprofit that collects and stores confidential information, Personally Identifiable Information (PII) or Protected Health Information (PHI) is vulnerable to a costly data breach and its consequences. Data breaches, denial of service attacks, and phishing scams are a sampling of methods that cybercriminals use to steal and extort data.

Organizations must remain vigilant and implement security protocols to safeguard their missions and critical data. However, establishing secure technology protocols and having best-in-class technology solutions isn't enough. Nonprofits shouldn't only focus their efforts on how to prevent cyber risks from materializing; they need to plan for *when* cyber threats happen. Restoring lost data and systems and responding to lawsuits resulting from breaches are potentially costly and time-consuming tasks; your response could tap critical funds and staff resources away from programs and services that are the lifeblood of your mission.

Consider the following statistics:

- Breaches affect organizations of all sizes and can be costly. The NetDiligence 2019 *Cyber Claims Study* reported 96% of claims were made by organizations with less than $2 billion in revenue, and

*CONTINUED ON PAGE 2*

**A PUBLICATION OF THE NONPROFIT RISK MANAGEMENT CENTER**
204 South King Street, Leesburg, VA 20175 | 703. 777.3504 | www.nonprofitrisk.org

*Risk Management*
ESSENTIALS

VOL. 29 • NO. 3 • FALL 2020
Published three times annually by the
Nonprofit Risk Management Center
204 South King Street, Leesburg, VA 20175
Phone: 703.777.3504
**www.nonprofitrisk.org**

Nonprofit
Risk Management
Center

**Staff Directory**
(All staff can be reached at 703.777.3504)

MELANIE LOCKWOOD HERMAN
Executive Director
Melanie@nonprofitrisk.org

KAY NAKAMURA
Director of Client Solutions
Kay@nonprofitrisk.org

KATHARINE NESSLAGE
Project Manager
Katharine@nonprofitrisk.org

WHITNEY CLAIRE THOMEY
Project Manager
Whitney@nonprofitrisk.org

## Demystifying Cyber Liability Insurance

CONTINUED FROM PAGE 1

a maximum breach cost in the nonprofit sector could be as much as $1.6 million.[1]

- It can take a long time to discover a breach. A study by IBM indicates that it can take as many as 280 days to identify a breach.[2]
- Breach containment response time is a critical factor in associated costs. Unsurprisingly, the size of the breach affects containment time; a mega breach can take up to 365 days to contain.[3]
- The average cost of lost records in 2019 was approximately $146 per record.[4]

Cyber Liability Insurance is an increasingly affordable option for financing the cost and consequences of a data breach. However, whether you decide to purchase—or forgo—this coverage, taking time to understand how the coverage works and what it covers is well worth the time required. At a minimum, nonprofit insurance buyers should understand what types of claims are covered, claim limits, and how to file a claim.

NRMC invited a panel of thought leaders from the insurance and legal industries to explore key questions, common misconceptions, and how to avoid mistakes when filing claims.
Our panel consists of:

- **Ryan FitzSimmons,** Divisional Vice President of Operations, Great American Insurance Group, Cyber Risk
- **Scott Konrad,** Senior Vice President and Not-for-Profit Practice Leader with Hub International Northeast, and member of NRMC's Corporate Advisory Committee
- **Keith Moulsdale,** partner and co-chair of the Cyber Security, Information Management & Privacy practice at Whiteford Taylor & Preston

## Q&A: What You Need to Know About Cyber Liability Insurance

### NRMC: What's the top misconception about cyber liability coverage?

**Ryan FitzSimmons:** A common misconception is that you automatically have enough cyber liability coverage as part of your commercial package or Business Owners Package (BOP). If you're looking for the most tested, most encompassing coverages in the marketplace, you need to purchase a stand-alone cyber risk product. Not all cyber endorsements to other insurance products are created equal. While there is some additional expense and effort involved with a stand-alone purchase, it's well worth it to ensure the limits and scope of coverage are adequate for your organization's needs.

**Scott Konrad:** Many charitable organizations assume they're improbable targets because they're too small, don't have information that would be valuable to cybercriminals, or they outsource certain technology. All are naïve assumptions.

Although some breaches occur because of technology lapses or criminal actions, a surprising number are attributable to simple human error. The duty to safeguard data is non-delegable--so that, even if an organization outsources payment or CRM functions, it's the one ultimately responsible to regulators and victims. The May 2020 Blackbaud breach poignantly illustrates how easily nonprofits can wind up in the soup for events they didn't even cause.

[1] https://netdiligence.com/cyber-claims-study-2019-report/

[2] https://www.ibm.com/security/data-breach

[3] https://newsroom.ibm.com/2018-07-10-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

[4] https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

CONTINUED ON NEXT PAGE

## Demystifying Cyber Liability Insurance

CONTINUED FROM PAGE 2

“Many charitable organizations assume they’re improbable targets because they’re too small, don’t have information that would be valuable to cybercriminals, or they outsource certain technology. All are naïve assumptions.”

**Keith Moulsdale:** It’s a common misconception that all cyber insurance coverage is created equally and that all policies cover both first- and third-party losses. In fact, there can be vast and material differences in cyber-related policies that can have a real impact on the policyholder. For instance, some policies only insure incidents that occur on a server that is owned or operated by the policyholder and don’t cover incidents that occur on servers hosted in the cloud or incidents that are connected to a vendor. With nonprofits moving rapidly to cloud-based solutions, this should be a key focus for organizations shopping for insurance.

Some policies don’t cover acts of cyber “terrorism” or “acts of war.” Those exclusions can be a real problem given the extensive and growing scale of incidents sponsored by nations such as Russia, China, and Iran, especially when the US or another Western government publicly recognizes that a particular hack was state-sponsored, such as in the case of the “NotPetya” cyber-attack in 2017 that was attributed to Russia.

Also, many cyber policies don’t cover phishing-related financial losses. Such losses occur when a fraudster gains access to an email system and then tricks someone in accounts payable into paying the fraudster instead of a legitimate vendor; those types of losses are more likely to be covered under a separate crime policy. Some policies cover governmental or third-party fines, but others don’t.

The list of possible material differences in policies goes on and on; this is why I routinely tell clients that perhaps the most important thing they can do when shopping for cyber liability coverage is to hire a broker that fully grasps the complexities and nuances of cyber risk. Ideally, this

CONTINUED ON PAGE 4

## Demystifying Cyber Liability Insurance

CONTINUED FROM PAGE 3

would be a broker specializing in such risk and who will suggest appropriate policies only after engaging in reasonable due diligence about the prospective policyholder's unique cyber-related first- and third-party risks.

### NRMC: What's the top mistake policyholders make when they have a claim?

**RF:** Too often, policyholders don't involve their carrier soon enough in the event of a claim. Time is of the essence in cyber claims management, and while it seems like you need to get things moving right away with lawyers and vendors and consultants, bringing that all together in the midst of a crisis is difficult at best. Most carriers have a pre-contracted list of top-notch vendors at the ready. With one phone call, you can bring all of those resources to bear and secure the most favorable rates from those experts. Your cyber carrier is your most significant resource. Don't go it alone.

**SK:** Some tend to panic and act without reading their insurance policy terms and conditions. Most policies have strict requirements governing notice to the insurer and gaining its prior consent to engage professional services or incur expenses. My strong advice is always to contact the placing agent/broker/risk advisor FIRST—and to be guided by its counsel; that intermediary can notify the insurer and mobilize resources.

**KM:** Three mistakes rise to the top of my list. One is failing to notify the insurer of a possible claim in a timely fashion. Failing to do so could cause the insurer to deny the claim.

Another common mistake is engaging lawyers or forensic specialists who aren't on the insurer's pre-approved list or have not been screened and approved by the insurer. Failing to get approval for the organization's preferred lawyer or other breach response professionals could cause fees and expenses charged by those professionals to be denied or limited.

But perhaps the biggest mistake of policyholders is trying to resolve an incident on their own without consulting with professionals who specialize in cyber incidents. Often, doing so entails a policyholder using a well-intentioned internal IT person to "remedy" an incident, but more often than not results in that person making mistakes that negatively affect the investigation, such as by reconfiguring logs in a way that actually deletes logs that include critical information about the incident.

### NRMC: What's the top uncovered claim that nonprofits submit?

**RF:** One of the top uncovered claims is fraudulently induced payments from socially engineered scams like business email compromise. Often, the limited scope of coverage in cyber endorsements does not include this feature unless you ask for it and pay the additional premium.

**SK:** For organizations that buy cyber protection, I actually haven't seen any non-covered losses! The state-of-the-art in policy design has advanced tremendously over the past 15 years, so that today's breed of products generally address (1) civil liability and regulatory matters, including defense, fines, and penalties; (2) breach response costs; and (3) first-party loss to the policyholder's own network and digital assets, including direct and contingent business interruption. Even economic loss from reputational harm is often covered, as is Multimedia Liability (for both online and offline content).

**KM:** The top uncovered claim that we see are claims for losses arising out of a so-called "business email compromise" where an employee or agent of the policyholder was tricked into sending money to a fraudster.

CONTINUED ON NEXT PAGE

## Demystifying Cyber Liability Insurance

CONTINUED FROM PAGE 4

> "...perhaps the biggest mistake of policyholders is trying to resolve an incident on their own without consulting with professionals who specialize in cyber incidents."

### NRMC: Who are the top carriers covering cyber losses for nonprofits?

**RF:** Given the frequency with which buyers are coupling their cyber risk insurance purchase together with other coverages, like their package policy or Directors & Officers (D&O) policy, it is likely that the top carriers covering cyber losses are also the leading writers of those other lines. However, as stand-alone products become increasingly available in the admitted marketplace, we expect to see movement toward specialty carriers to accelerate.

**SK:** There are over 100 markets playing in the space: a combination of the household-name mega-players and newer niche specialists. Everyone's vying for market share, and the cyber segment is one slice of today's turbulent market that's remained intensely competitive. Every broker has its favorites, but we've had great success with companies such as Beazley, Chubb, and AIG for stand-alone policies, and Travelers and Zurich when bundling Cyber with other companion lines such as Management Liability and Crime. There's certainly no shortage of options.

**KM:** There are a growing number of good cyber liability and loss carriers, but I routinely see suitable policies offered by Axis, Chubb, CNA, and Travelers.

Whitney Thomey is Project Manager at the Nonprofit Risk Management Center. She welcomes your follow-up questions about any of the topics covered in this article at 703.777.3504 or Whitney@nonprofitrisk.org.

Nonprofit
Risk Management
Center
Find the answer here | nonprofitrisk.org

# Consulting Services

**COMPETENCE** **CONNECTIONS** **CONFIDENCE**

**The Nonprofit Risk Management Center is committed to supporting your nonprofit through periods of transition, expansion and transformation.**

**You're looking for specialized risk expertise because:**

- **Your team needs a best-in-class risk management program that positions your mission for growth and continued success**
- **The Board has requested that your organization adopt an Enterprise Risk Management program**
- **A near-miss, serious incident or lawsuit has led you to wonder what you don't know**

## WE PROVIDE

**Resources and Expertise** that are custom, fresh, and never recycled

**25 Years of Experience** as a trusted advisor to mission-driven organizations

**Custom Support and Advice** when and how you need it

**Fixed-Fee Cost Structure**

## WE DELIVER

- An independent assessment to provide a broader perspective on your critical risks and changing risk landscape
- A direct line to our team of nonprofit risk specialists to guide you through your toughest risk challenges
- Clear, practical advice and recommendations to achieve your risk management goals and objectives
- Clear, expert guidance to help you build a sustainable, integrated, mission-advancing risk function

**FIND THE ANSWER HERE | NONPROFITRISK.ORG**
204 South King Street, Leesburg, VA 20175 | Phone: 703.777.3504

# Case Studies

## 1 Engagement Goal: Elevating and integrating ad-hoc conversations about risk-taking and risk management into durable planning and decision-making processes

**WHO:** A national foundation working to strengthen democracy and promote the health, diversity, and resilience of democratic processes and institutions.

**Results:** The NRMC team worked in partnership with foundation leaders to identify and unpack critical risks. The project culminated with a workshop exploring the topics of risk assessment and risk appetite. The NRMC team will be returning to the organization later this year to facilitate follow-up training for a broader staff team.

## 2 Engagement Goal: Interim Risk Leadership

**WHO:** A regional transit agency employing more than 1,200 staff.

**Results:** The engagement involved leading and motivating staff working in claims management and safety and partnering with the agency's top executives to envision a new structure for the risk team. NRMC's work included managing contacts with the agency's external broker and defense counsel and facilitating the vetting and appointment of a new Third-Party Administrator (TPA). The NRMC team also led the search process for a new risk leader and developed a new risk dashboard to elevate and strengthen risk oversight.

## 3 Engagement Goal: Development of an engaging website housing custom risk resources for the organization's member agencies

**WHO:** A national organization of 1,000 affiliated agencies dedicated to fighting poverty in the U.S.

**End Result:** The NRMC team developed an attractive website featuring two interactive web applications. These applications present content fully customized for the association. The site also has easily accessible web links to NRMC Affiliate Member benefits. These resources help the organization's affiliated agencies develop a deeper awareness of the risks they face and identify practical steps to close gaps in risk practice. More than 95% of the organization's affiliated agencies have used the site to complete a Risk Assessment and demonstrate compliance with national quality standards.

## 4 Engagement Goal: Thoughtful bidding process to identify and select the best-qualified firm to provide insurance

**WHO:** A regional public health organization with more than 1,700 employees serving nearly 200,000 consumers.

**End Result:** The NRMC team facilitated and managed a Broker Selection Process for the agency motivated by the commitment to ensure that insurance dollars were allocated wisely. The NRMC team designed a custom RFP, identified and pre-qualified bidders, reviewed incoming proposals based on the client's criteria, and coordinated interviews with the six finalist firms. At the end of the process, the client selected a new broker and entered into a multi-year broker services agreement.

**FIND THE ANSWER HERE | NONPROFITRISK.ORG**
204 South King Street, Leesburg, VA 20175 | Phone: 703.777.3504

# Know Your CyberSpeak: A Cyber Risk Glossary

Navigating the world of cyber risk often feels a lot like learning a foreign language. Terms and concepts can be confusing and unfamiliar. This Cyber Risk Glossary will help nonprofit leaders as they examine cyber liability insurance policies and develop the necessary technology-related security protocols to protect their missions.

**Cloud –** The term "Cloud" refers to a product created and hosted by a third party and accessible via the internet. Cloud products range from data storage solutions such as OneDrive and Dropbox, to communications tools such as Gmail, and software and productivity products such as Microsoft Office or Google Docs. Cloud products can generally be customized, adapted, and arguably 'managed' in house by an end user or a nonprofit's IT team. Many organizations view cloud-based products as a key to business continuity; if servers and systems at a nonprofit are damaged or otherwise inaccessible, systems and data stored 'in the cloud' should still be accessible by a user with an Internet connection and an authorized login.

*Cloud Risks: It's risky to assume that the cloud solves all your storage and redundancy problems! Peruse "Cloud Computing – BCP Boon or Boobytrap?" to review how to manage the risk of getting lost in a technology fog.*

**Cyber Resilience –** Nonprofits that practice cyber resilience work to prevent cyber-attacks while accepting that not every attack is avoidable. Resilient organizations implement strategies that provide rapid recovery and response methods and manage downside events and outcomes to mitigate losses and ensure continuity of operations.

**Cybersecurity –** Cybersecurity is a collection of technology, processes, and practices that focus on protecting electronically stored information from theft or damage. The NIST Cybersecurity Framework, released in 2014, is one of the best-known cybersecurity frameworks and is structured as a series of stages: prevention, detection, and response. Cybersecurity's focus is broader than its counterpart, data security. Nonprofits should use this framework to protect networks and infrastructure from attacks, disruption, misdirection, and bad actors.

**Data Security –** Data security is the narrower arm of cybersecurity. In this discipline, nonprofit information technology specialists focus on protecting

CONTINUED ON NEXT PAGE

## Know Your CyberSpeak: A Cyber Risk Glossary

CONTINUED FROM PAGE 8

the data stored by organizations, for example, keeping names, social security numbers, and payment information secure. Data security policies and procedures center on keeping unauthorized individuals from acquiring personal information—either from a data breach or even a lost laptop.

**Encryption key –** An encryption key is a random string created by an automated security algorithm to secure and protect information. Encryption keys can be used to secure data that needs to be sent to other parties. The key is used to scramble data and unscramble data when the authorized party has received it and is ready to view it. Computer-generated algorithms ensure the key is randomly generated and unique, making it more difficult for hackers to crack.

**Internet of Things (IoT) –** Internet of Things (IoT) is the general term used to capture the growing number of devices able to connect to the internet and provide "use" data. In recent years, the IoT has expanded beyond computers and cell phones to include "smart" appliances and speakers, health care equipment, security cameras, thermostats, and many other devices. These devices capture many different types of data, some more sensitive than others. Because they don't rely on human intervention to function, they can fall victim to being set up and forgotten about. Each IoT device provides another potential access point for bad actors to access the network and/or the data it connects to.

*IoT Risks: IoT allows nonprofits to harness "big data" and automate areas that previously required valuable staff time. The risk of a data breach can be more significant if proper measures aren't established to protect data and automated sensors. Learn more about cyber threats and security protocols for the IoT from Deloitte's article "Cyber Risk in an Internet of Things World."*

**Malware –** A catchall term for any piece of software that changes the behavior of a computer, website, application, or other device which causes harm. Examples of malware include viruses, keyloggers, ransomware, and other malicious programs. Often malware is used to collect sensitive information such as credit card or social security numbers, or to disrupt the everyday use of a network by shutting down servers or making web pages unusable.

**Phishing –** Phishing scam emails are composed and sent to trick the receiver into revealing sensitive information such as employee IDs, usernames, and passwords. Scammers often encourage the receiver to click on a link that leads to a website controlled by a hacker; these false websites may look convincingly like the sites they are mimicking.

**Ransomware –** Ransomware is a specific type of malware that infects a system and then encrypts all of the user's information. The user is then instructed to pay for the encryption key to avoid losing their data or access, often through a cryptocurrency such as bitcoin.

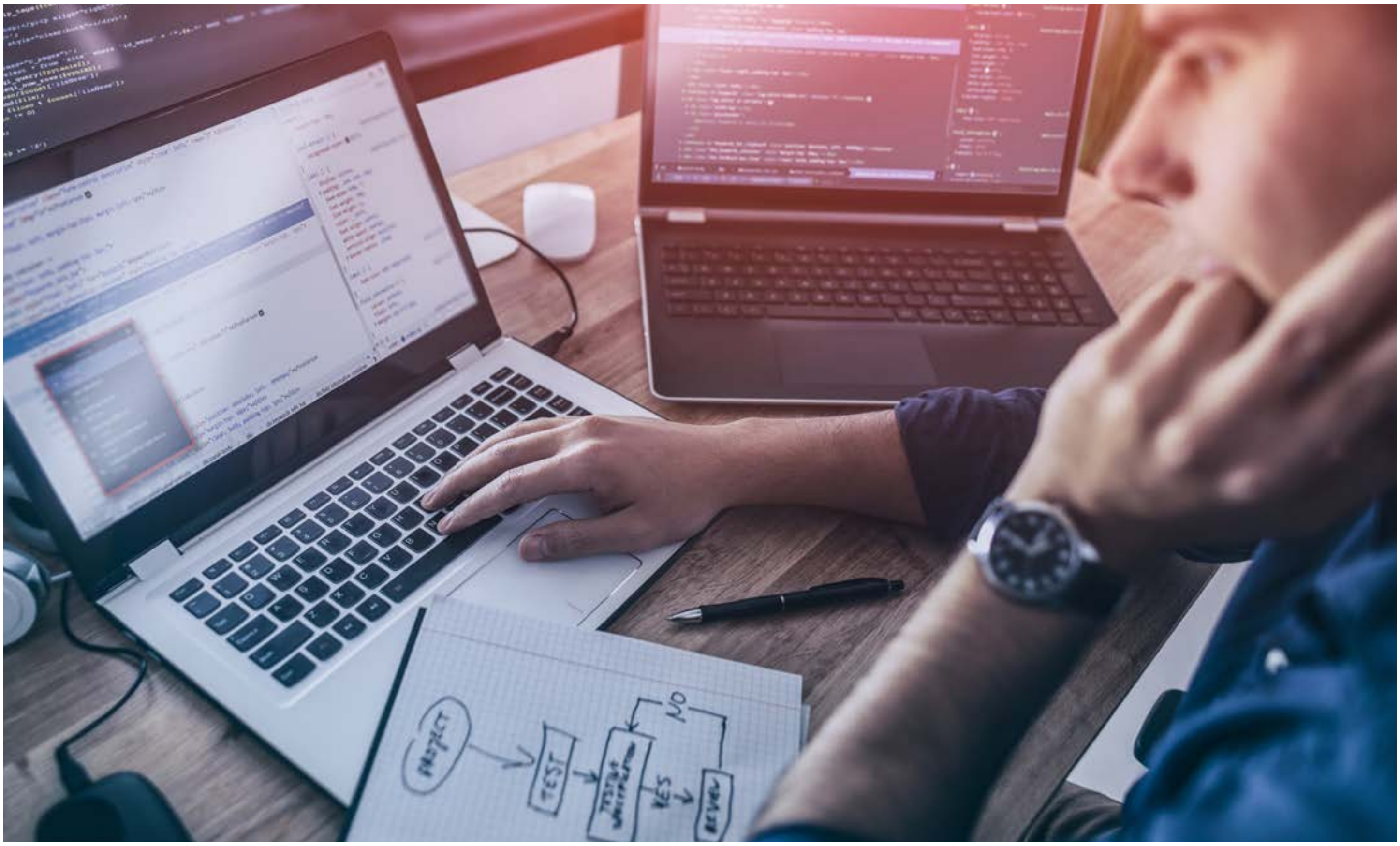
**Social Engineering –** Social engineering is the act of manipulating a person into providing confidential information. Many phishing attempts use social engineering to encourage the receiver to trust the email's author and provide the requested information. Pretexting is another method of social engineering, but generally involves a malicious actor attempting to trick, cajole, or threaten someone into revealing sensitive information over the phone.

**Two-Factor Authentication (2FA) –** An extra layer of security where access to a user is only granted once they have provided a secondary form of identification after providing their initial username and password. Two-Factor Authentication usually requires a user to prove that they are the owner of an email account, cellphone, or other device where one-time access codes are sent or generated and then provided as proof that they have the permissions to access the protected application or device. Multi-factor authentication (MFA) requires two or more independent credentials. An easy way to remember what MFA means is that it requires 1) something you "know,' such as a password, 2) something you 'are,' such as a form of biometric recognition, and 3) something you 'have', such as a security token.

*2FA Risks: Two-Factor Authentication does provide an added layer of security for access to sites storing sensitive data. However, nonprofits should be vigilant when selecting and updating access devices as staff leave their roles at the nonprofit. Critical access could be denied if the access device (a cell phone or alternate email address) is no longer available.*

**Virtual Private Network (VPN) –** An encrypted pathway through the internet that allows a user to access a primary network from a remote location. VPNs are commonly used to enable employees to access office systems from home, and often require two-factor authentication or other layers of security before a secure connection is established.

*VPN Risks: Virtual Private Networks are excellent avenues to connect staff with essential software and data. However, the COVID-19 pandemic has exposed additional risks nonprofits should consider when utilizing VPNs for work-from-home staff members. Often home networks are insecure, making VPNs more vulnerable to hackers and bad actors.*



# Framework to Implement a Cybersecurity Plan

*By Afua Bruce for NTEN*

Once organizations understand what cybersecurity is and recognize that it is a threat to their operations, the next step is to assess what cyber risks the organization has. By conducting risk assessments and implementing appropriate protections, organizations can decrease the likelihood of a cybersecurity attack. Additionally, the risk assessment process often increases communication within an organization, at least temporarily, since those facilitating the assessment must speak to employees throughout the organization.

Although many risk assessment guidelines exist, standards based on the National Institute of Standards and Technology (NIST) guidelines are generally considered the best. The NIST Cybersecurity Framework includes five functions[1]:

- **Identify** cybersecurity risks
- **Protect** against potential cybersecurity events
- **Detect** cybersecurity events
- **Respond** to a cybersecurity incident
- **Recover** from a cybersecurity incident

Nonprofits, especially, should be concerned about three categories of risks and threats:

- Reputation – that an account will get compromised to send spam
- Financial – an employee, volunteer, or donor will be tricked into sending money
- Distraction – an employee's system will be compromised through automated tooling, which can cause organizations to deal with disabled systems, ransomware, or wonder what was actually accessed; this all costs a great deal of work and money

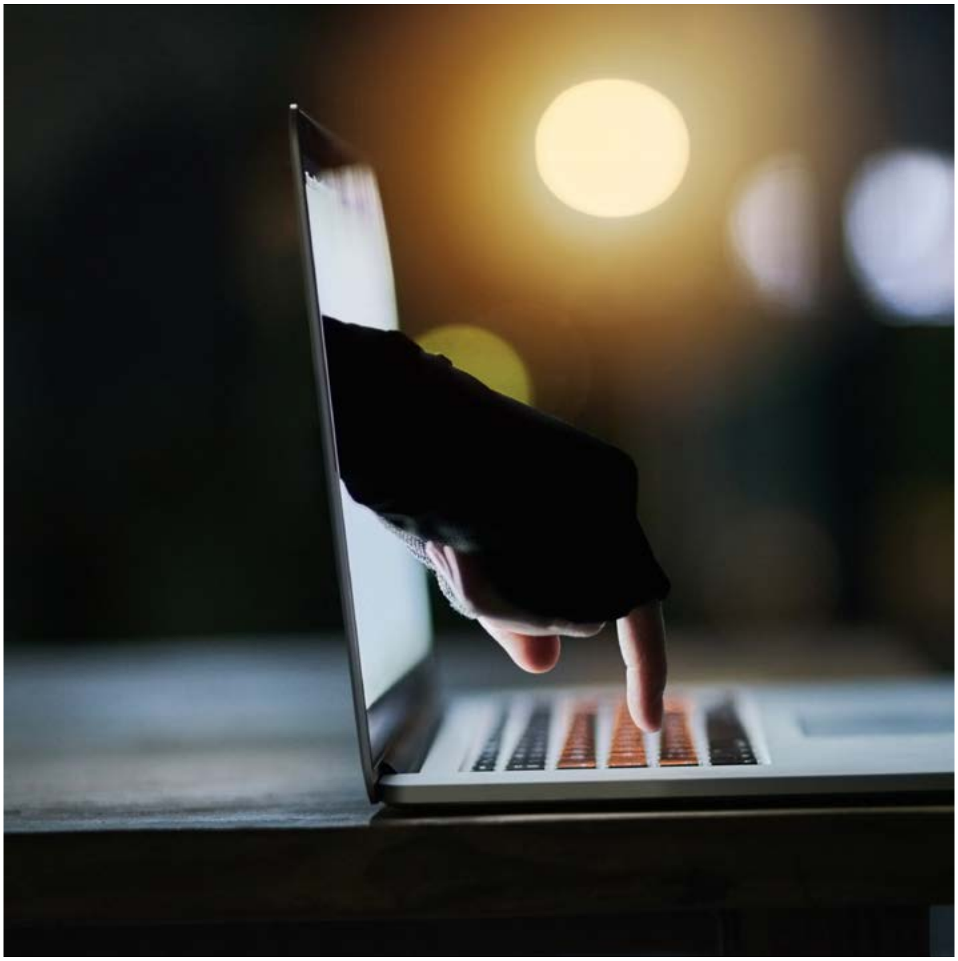
To further understand what risks an organization may face, the organization must first begin by identifying the data it collects. NIST defines risk assessments as tools "used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems." To perform a risk assessment, begin by listing all

[1] Cybersecurity Framework: The Five Functions. https://www.nist.gov/cyberframework/online-learning/five-functions

*CONTINUED ON NEXT PAGE*

## Framework to Implement a Cybersecurity Plan

CONTINUED FROM PAGE 10



> "Should an organization fall victim to a cybersecurity attack, the primary goal in responding to the incident is to contain, or prevent the spread and impact, of the attack."

data the organization collects and uses, and then asking who, where, what, and how. For each data type, determine 1) who owns the data, 2) where the data is stored, 3) what the level of sensitivity or confidentiality of the data is, and 4) how access controls and security measures are implemented on the data. Organizations will need to repeat this process for other digital and physical assets, including websites and servers; these assets are vulnerable to cyber-attacks as well. The next step in this process is, for each item on the list, to determine the impact of a cyber breach or attack, and the likelihood of an attack.

The protect step of the framework "supports the ability to limit or contain the impact of a potential cybersecurity event."[2] This includes activities such as training staff on cybersecurity awareness, creating policies and procedures to protect systems and data, and strengthening access control by requiring strong passwords and controlling who has access to data and when. Protecting against potential cyber events translates to proactively implementing security protocols to make an organization's systems and data more difficult for attackers to access. Detecting cybersecurity events is more challenging, as "cybersecurity incidents are often difficult to detect."[3] In fact, attackers reside within a system on average 146 days before being detected.[4] To effectively carry out this function, organizations should

[2] Cybersecurity Framework: The Five Functions. https://www.nist.gov/cyberframework/online-learning/five-functions

CONTINUED ON PAGE 12

## Framework to Implement a Cybersecurity Plan

CONTINUED FROM PAGE 11

> “Protecting against potential cyber events translates to proactively implementing security protocols to make an organization’s systems and data more difficult for attackers to access.”

implement continuous monitoring software to alert organizations of any anomalies in the system.

Should an organization fall victim to a cybersecurity attack, the primary goal in responding to the incident is to contain, or prevent the spread and impact, of the attack. Organizations will need to communicate with a variety of internal entities, including legal, HR, and IT, and external entities, including law enforcement, clients, and donors, as appropriate. Organizations must also analyze how hackers were able to access the system, and update protocols to prevent future attacks. Recovering from a cybersecurity attack requires organizations to restore functionality to the pre-attack state. Organizations that regularly backup data and systems will have an easier time restoring information and operations.

The NIST Cybersecurity Framework is intended to scale with an organization’s resources. All organizations should develop the capability to periodically conduct cybersecurity risk assessments, and identify, at least theoretically, steps to be taken if any data or systems are compromised. Using the risk assessment to guide conversations between an organization’s IT, finance, programs, and executive leadership, will allow the organization to understand its vulnerabilities and make informed decisions about how much risk to absorb, and how many resources should be expended to mitigate the remaining risks.

*This excerpt was originally published by NTEN. Risk Management Essential readers can read the full copy in “Cybersecurity for Nonprofits: A Guide.” NRMC received permission from NTEN to republish this excerpt.*

[3] Microsoft Inc. Nonprofit Guidelines for Cybersecurity and Privacy. https://download.microsoft.com/download/1/D/4/1D494A7D-D153-40FC-BC18-F4C2F800E752/Nonprofit_Guidelines_for_Cybersecurity_and_Privacy.pdf

[4] Microsoft Inc. Advanced Threat Analytics. www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/advanced-threat-analytics

# What Your Board Needs to Know About Cyber Threats

*By Melanie Lockwood Herman*

Risk is top-of-mind for many nonprofit boards these days. Board members understandably want to grasp the top risks facing an organization and have confidence that the management team is prepared to weather the downside risks it cannot avoid. And based on our work with nonprofits across a wide spectrum of missions, the risk of a data breach occupies a spot on most 'top 10 risks' list.

What should a board be asking, talking about, and focused on when it comes to data breach risk and cyber threats? How can management teams keep their boards apprised of cyber threats without opening the door to unproductive excursions into day-to-day management and operations?

## Key Cyber Risk Discussion Topics for the Board

The NRMC team recommends being proactive in educating your board about cyber threats and the strategies you have established to mitigate the risk of a data breach. How? Anticipate the questions board members are likely to ask and prepare thoughtful, responsive answers. We hope the following questions will be helpful as you prepare to engage with your board on a tricky but timely topic.

- **What is the risk of a data breach?** Education-focused topics are becoming standard components of nonprofit board agendas. Board members increasingly recognize that deepening their understanding of critical issues is key to discharging their fiduciary and governance roles. Consider inviting a third-party expert to brief the board on the evolving landscape of cyber threats and data privacy. An educational segment is an excellent precursor to sharing information on what your nonprofit is doing to mitigate the risk of a breach.
- **What is the organization's exposure to cyber threats and data breaches?** Segue from a general briefing on the landscape of cyber threats to how these threats potentially impact your nonprofit. For example, explain how and why your agency collects and uses Personally Identifiable Information (PII) or Protected Health Information (PHI). When describing your exposure to privacy breaches, remember to

CONTINUED ON PAGE 14

## What Your Board Needs to Know About Cyber Threats

CONTINUED FROM PAGE 13

> "Because cyber risk is present for nearly every nonprofit, leaders should work with their boards to establish a transparent reporting process that will allow the board to effectively discharge their oversight role."

humbly acknowledge that data is at risk from third-party attacks as well as insider missteps!

- **What strategies are in place to guard against the risk of a data breach?** Share an overview of the myriad strategies your team has adopted to reduce the likelihood of a breach, detect a breach quickly, and reduce the overall cost and disruption of a breach. Keep in mind that merely saying that "we've backed everything up" won't convey readiness to cyber-savvy board members, nor is "backing up" a robust strategy.
- **What will we do if we experience a data breach or attempt to access protected or confidential information?** Describe the strategies and approaches you've put in place to respond upon learning of a potential or actual data breach. Explain third-party advisors' roles, such as counsel, loss control reps at your insurance carrier, or IT consultants. Also, provide an overview of how your cyber liability policy, if you have one, is expected to support your response and the extent to which the policy will cover some of the financial aspects of a breach. Be sure to clarify what the policy doesn't cover. Depending on your coverage, those exclusions might be acts of war, loss of equipment, failure to implement security measures, and loss of future revenue, among others.
- **What is the cost of the protections and cybersecurity strategies we have put in place?** The board will want to understand and gauge whether your nonprofit has made an appropriate investment in protective and preventative strategies. Be prepared to describe the staff time commitment, the investment in tools and tech protections, and the scope and cost of your cyber liability insurance policy.

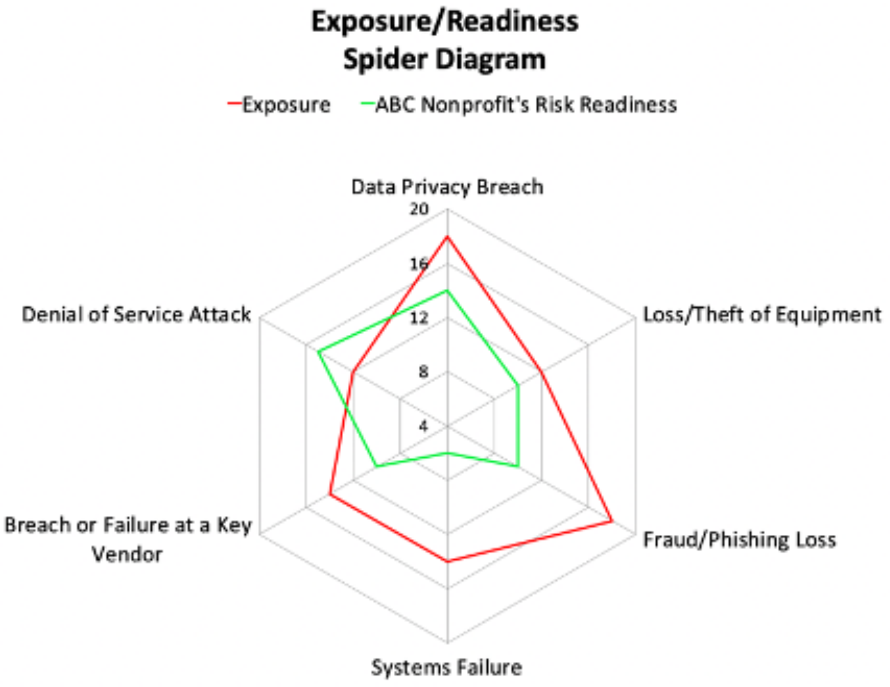
### Make it Visual

Today's management teams are increasingly using dashboards and graphics to illustrate progress towards goals, financial health, and more. A risk dashboard

CONTINUED ON NEXT PAGE

## What Your Board Needs to Know About Cyber Threats

CONTINUED FROM PAGE 14



or maturity model is a potentially useful tool to exhibit how your team is evolving its risk management practices related to cyber threats.

For example, using the Radar option in Excel, you can create a Spider Diagram contrasting the perceived threat of a data breach to your nonprofit's 'readiness.' The diagram shows where the most significant gaps lie and opportunities for further investment. In the example below, the greatest gaps between exposure and readiness are in two areas: systems failure and fraud/phishing loss. Sharing a visual such as the one below could be helpful if an upcoming board decision relates to allocating additional resources to close the gaps.

Because cyber risk is present for nearly every nonprofit, leaders should work with their boards to establish a transparent reporting process that will allow the board to effectively discharge its important oversight role. The NRMC team hopes that by using the education, discussion, and reporting tips presented in this article you will be able to empower your board to strengthen its oversight role, including its focus on how cyber risks could impact your organization's strategic objectives.

Melanie Lockwood Herman is the Executive Director of the Nonprofit Risk Management Center. She welcomes your questions about the board's risk oversight role NRMC's consulting services at 703.777.3504 or Melanie@nonprofitrisk.org.

## Additional Resources on Boards and Cyber Security

"How Much Do Nonprofit Board Members Need to Know About Cybersecurity" - www.boardeffect.com/blog/how-much-do-nonprofit-board-members-need-to-know-about-cybersecurity/

"Staying Cyber Aware in a Crisis: Smart Tips for Nonprofit Boards" - www.boardeffect.com/blog/staying-cyber-aware-crisis-smart-tips-nonprofit-boards/

"3 Questions Boards Want Answered About Cyber Security" https://symantec-enterprise-blogs.security.com/blogs/feature-stories/3-questions-boards-want-answered-about-cyber-security

"Cybersecurity: Emerging challenges and solutions for the boards of financial-services companies"www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-emerging-challenges-and-solutions-for-the-boards-of-financial-services-companies

"What Boards are Doing Today to Better Oversee Cyber Risk," www.ey.com/en_us/board-matters/what-boards-are-doing-today-to-better-oversee-cyber-risk

RISK MANAGEMENT MARKETPLACE

At Care Providers Insurance Services, our nonprofit insurance experts have been serving those who serve our communities for more than 25 years. We understand the unique needs and critical coverages for nonprofits and social service organizations, delivering specialized insurance programs and support — from robust coverage and competitive pricing, to best-in-class customer service and dedicated underwriters and claims managers. Because with the right partner in place, you can focus less on your insurance ... and more on your mission.

ID/DD Organizations • Youth Mentoring • Religious Institutions • Charter Schools • Community Action Agencies

Call (833) 700-0097
Or Visit **Info.INS-CPS.com**

**Care Providers**
Insurance Services

A Program Built by NSM Insurance Group

Inclusion in the Marketplace does not constitute an endorsement by the Nonprofit Risk Management Center. To inquire about space availability, contact Kay@nonprofitrisk.org

HUMAN SERVICES PROTECTION NON-PROFIT/FOR PROFIT

## MILLIONS OF PEOPLE SERVED. 1 SHARED RESPONSE.

PHLY helps ensure that our Human Services customers continue to gain positive feedback from the millions of people they serve. We offer customizable package policies, along with superior customer service, and a free risk management plan toolkit to help meet the ever growing needs of non-profits.

AM Best A++ Rating

Ward's Top 50 2001-2018

96.1% Claims Satisfaction

100+ Niche Industries

Call 800.873.4552
Or visit Think**PHLY.com**/HumanService

PHILADELPHIA
INSURANCE COMPANIES

A Member of the Tokio Marine Group

Non-Profit /For Profit Human Services | Mental Health | Substance Abuse | Home Health Care | Home Medical Equipment

Philadelphia Insurance Companies is the marketing name for the property and casualty insurance operations of Philadelphia Consolidated Holding Corp., a member of Tokio Marine Group. All admitted coverages are written by Philadelphia Indemnity Insurance Company. Coverages are subject to actual policy language.

Inclusion in the Marketplace does not constitute an endorsement by the Nonprofit Risk Management Center. To inquire about space availability, contact Kay@nonprofitrisk.org

# JOIN US

## AT OUR UPCOMING EVENT

COMPLIANCE | HR | SAFETY | STRATEGY | TRENDS | TECHNOLOGY | INSURANCE

## APRIL 12, 2021

NONPROFIT ERM SYMPOSIUM

### NONPROFIT ERM SYMPOSIUM

A brand-new Enterprise Risk Management (ERM) educational event for experienced risk leaders. This day-long Symposium will be presented as a hybrid event; attend in-person or stream live sessions from the comfort of your home or office. Explore and learn ERM strategies through workshops and small cohort discussion groups.

**Topics include:**

- ERM in the Nonprofit Sector: A Guided Tour
- Five Characteristics of a Successful, Mature ERM Program
- Sync Your ERM Goals, Aspirations and Framework to Your Nonprofit's Values
- Roundtable: Ways that ERM Has Transformed My Organization
- Right-Sizing Risk Reports Based on Audience Wants and Needs
- **And Much More...**

FOR INFORMATION AND TO REGISTER, VISIT **NONPROFITRISK.ORG/EVENTS**

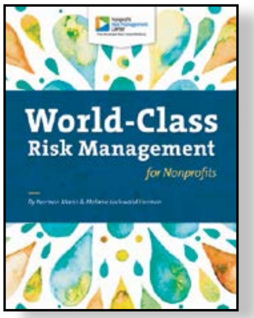
Nonprofit
Risk Management
Center

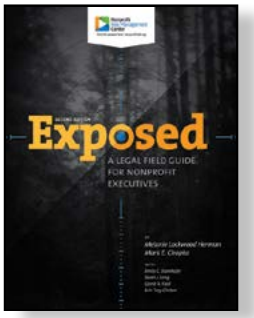
NRMC is a 501(c)(3) nonprofit with a mission to inspire effective risk management practices and Risk Champions.

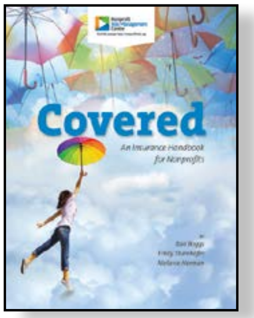
Nonprofit
Risk Management
Center

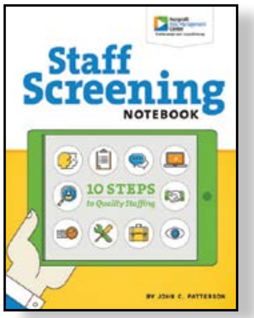
find the answer here | nonprofitrisk.org

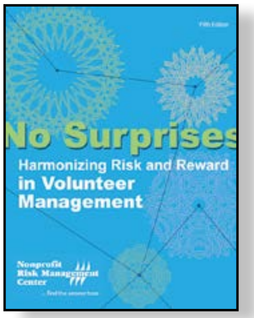
## Your risk management reading list starts at nonprofitrisk.org/products

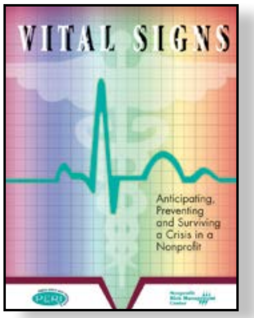


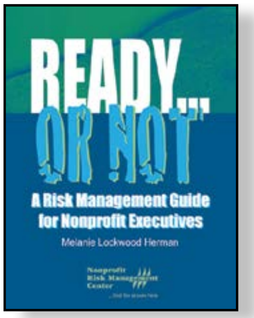







Fifth Edition
No Surprises
Harmonizing Risk and Reward in Volunteer Management
Nonprofit Risk Management Center


Vital Signs
Anticipating, Preventing and Surviving a Crisis in a Nonprofit



Interested in purchasing 10 or more books?
Contact Kay at 703.777.3504 for bulk pricing

**FIND THE ANSWER HERE | NONPROFITRISK.ORG**
204 South King Street, Leesburg, VA 20175 Phone: 703.777.3504

Nonprofit
Risk Management
Center

204 South King Street
Leesburg, VA 20175

# Risk Management ESSENTIALS

Tips, Knowledge and Tools for Nonprofit Organizations

## PLEASE ROUTE TO:

□ **Executive Director**
□ **Director of Volunteers**
□ **Risk Manager**
□ **Legal Counsel**
□ **Human Resources**
□ **Finance/Administration**

## INSIDE THIS ISSUE

## NEW AFFILIATE MEMBERS

Learn more about NRMC's Affiliate Member program at nonprofitrisk.org/affiliate-membership. NRMC would like to welcome our new Affiliate Members.

Center for Developmentally Disabled

Facing History and Ourselves

University of Missouri - Midwest Center for Nonprofit Leadership

YWCA