FOUR PILLARS OF CYBER-RISK MANAGEMENT FOR NONPROFITS

PARTNERS
IN REGULATORY COMPLIANCE

I. FOUR PILLARS OF CYBER-RISK MANAGEMENT FOR NONPROFITS

Following the delayed notice of a ransomware attack on fundraising technology vendor Blackbaud, the nonprofit industry is reassessing its approach to cyber-risk management in the COVID era.

Cybercriminals breached Blackbaud, one of the world's largest providers of cloud-hosted fundraising software for nonprofits, in early February. But the company didn't uncover the breach until mid-May, following a suspicious login on an internal server [1].

The fact that Blackbaud waited until mid-July to disclose the breach is what has their nonprofit clients flummoxed. Although threat actors managed to exfiltrate a copy of a database subset from Blackbaud's self-hosted environment, company representatives assured their customers that no credit card data, bank account details, or social security numbers were stolen.

Blackbaud representatives told the Nonprofit Times they recreated and tested the cyberattack internally via a third-party cybersecurity firm to ensure that customer data was still intact. But the company and its clients are still assessing the full extent of the exploit. Blackbaud said it 'resolved' the issue in late June after paying the attacker a bitcoin ransom of unknown value.

Even though this breach is more illustrative of a vendor risk scenario, nonprofits of all sizes, but particularly smaller organizations with less robust budgets for IT spend, find themselves increasingly vulnerable to a cybercrime contagion that has proliferated alongside the pandemic.

[1] https://www.thenonprofittimes.com/npt_articles/the-hack-of-blackbaud-damage-is-still-being-assessed/

Furthermore, the consequences of a data breach can be catastrophic for smaller social-good organizations. A cyberattack could threaten business interruption, reputational damage, and the exposure of employees' and donors' personal, health and, legal data. This can lead to the loss of donor relationships, business failure, and even the threat of regulatory enforcement.

Today, the top threat stalking the enterprise is the same attack that hit Blackbaud: Ransomware. This scourge alone costs American small businesses an estimated $75 billion per year, according to cloud management firm Datto [2]. This is an exploit where cybercriminals sequester enterprise data through email phishing attacks that trick people into downloading malicious links and attachments.

Once people click on or download infected documents, contaminated files implant malicious software, or malware, into victim networks. This type of malware is programmed to encrypt victim data and hold it hostage until a bitcoin ransom is paid.

If victims are dealing with 'honest' hackers, crooks will provide them with a functional decryption key to unlock their precious data. But the keyword here is "functional," and contractual compliance is far from a given in underworld agreements. When you consider that large enterprises typically report between 10-million and 99-million records compromised per data breach, according to cloud security firm Iomart [3], the consequences for smaller nonprofits can escalate into matters of life and death.

According to Datto's 2019 Global State of Ransomware Report, 45 percent of managed services providers (MSPs) say data-ransom attacks cause "business-threatening downtime" [4] for their small-business clients. Additionally, Datto reported that the average cost of ransomware

[2] https://www.datto.com/news/american-small-businesses-lose-an-estimated-75-billion-a-year-to-ransomware
[3] https://blog.iomart.com/cost-of-a-data-breach
[4] https://www.datto.com/resource-downloads/Datto2019_StateOfTheChannel_RansomwareReport.pdf

attack downtime for small businesses last year was $141,000. That's a 200-percent increase from 2018, Datto says.

Beyond ransomware, cybercriminals are increasingly pilfering employee credentials or impersonating vendors to perpetrate business email compromise (BEC) fraud, tricking employees into fulfilling fraudulent wire and invoice requests. BEC fraud spiked by 200 percent between April and May of this year, according to cyber-defense firm Abnormal Security [5].

With Iomart reporting that data breaches are up 273 percent from last year, nonprofits must be vigilant. Cyberthreats are amplified by the pandemic-induced business disruption that has forced enterprises to increasingly migrate to remote-work environments. As such, the enterprise attack surface has mushroomed, and nonprofit data has never been more at risk.

Regulatory risk is also rising. In addition to Europe's General Data Protection Regulation (GDPR), emerging cyber-regimes in California and New York are raising the stakes for organizations. [6]

But this is no reason to panic. Combining regulatory diligence with the Nonprofit Technology Network's three-step guide to launching a cybersecurity program, organizations can insulate themselves from rising threats .

Thus, the four pillars of cyber-risk management are: Conducting a holistic IT assessment of all enterprise data and network devices, threat-modeling all known attack vectors, identifying the regulatory regimes that could subject them to various types of enforcement actions, and forming an incident-response plan for the discovery of a breach, which has become increasingly inevitable.

In this white paper, Partners in Regulatory Compliance will provide an intuitive guide for nonprofits to enhance their cybersecurity controls, with a focus on the nature of risk and corresponding regulations in a changing business environment.

[5] https://www.techrepublic.com/article/2020-sees-rise-in-invoice-and-payment-fraud-bec-attacks/
[6] https://www.nten.org/article/assessing-risk-protect-valuable-data/

II. IT ASSESSMENT

NTEN advises nonprofits to create an inventory of all the data assets, networked devices, and operating environments that comprise the nonprofit enterprise. Organizations need to have a firm understanding of the type of data they possess, all the storage repositories and devices where it can be located, and "most importantly," its level of sensitivity, according to NTEN.

"List all of the different types of data by location. For example, if you have a donor management system, list everything it collects and stores: addresses, donations given, petitions signed, etc. Then, move on to your website and list everything stored on it," advises NTEN[6].

Additionally, organizations need to repeat this process for every database where information is stored, with an emphasis on cloud environments. While smaller nonprofits are less likely to have the complex and sprawling cloud arrangements that one might expect from organizations like Goodwill or the Salvation Army, they will also be less informed on cloud-security hygiene. This makes smaller nonprofit organizations especially vulnerable.

Having a simple, organized filing system to index data assets, their whereabouts, and their level of value is essential for this process. This spreadsheet[7] template can help simplify the audit. Once organizations have mapped out the lay of the proverbial land in their data environment, NTEN recommends segregating data into the following three categories [6]:

- **Data that cannot be lost**
- **Data that cannot be exposed**
- **Nonessential data**

Data-loss prevention concerns will vary by nonprofit organization. However, nonprofit data exposure risks generally center on donor information, human resources records, payment data, and certain internal emails. As for non-essential data, this too will vary by organization. However, designating data as nonessential does not give organizations carte blanche to be careless with it, advises NTEN. Nonessential simply means that organizations are not "going to place a high priority on securing it," NTEN says.

One last thing that nonprofits should consider in their IT assessment is the issue of technical debt. Organizations need to determine just how current their technology assets are. Antiquated tech obviously heightens vulnerabilities for nonprofit organizations. Now that the IT audit is complete and the enterprise cyber-environment has been mapped out and indexed by location and significance, the next step in the process is the threat model.

[7] https://docs.google.com/spreadsheets/d/1L1FP-ePpPLcrkYKKQkuLdFHV6xj9Y-k6z4jaBQKxgKE/edit#gid=0

III. THREAT MODELING

According to CSO Online, threat modeling is "a structured process through which IT pros can identify potential security threats and vulnerabilities, quantify the seriousness of each, and prioritize techniques to mitigate attack and protect IT resources [8]."

There are roughly seven generally accepted threat-modeling standards. One commonly used methodology that nonprofits should explore is the U.S. National Institute of Standards and Technology (NIST) framework. NIST breaks down the enterprise threat model into four steps:

- **Identify and characterize the system and data of interest**
- **Identify and select the attack vectors to be included in the model**
- **Characterize the security controls for mitigating the attack vectors**
- **Analyze the threat model**

This NIST draft provides nonprofits with a detailed guide illustrating how this threat-model framework would be implemented in practice [9]. However, nonprofits may be able to keep their threat audit slightly simpler. NTEN distills the process into three simple questions that all nonprofits should ask themselves when modeling [6]:

- **What could happen to that data?**
- **How likely is it that something would happen to it?**
- **How bad would it be if something happened to it?**

We already cited ransomware and some of the other the leading cyber-threats facing the modern enterprise in the introduction, but, overall, the risks are innumerable. NTEN highlights the following as some of the most common pitfalls for nonprofit organizations:

- **Physical theft of equipment or confidential files**
- **Natural disaster**
- **Inappropriate use of software**
- **Phishing (employees fooled into providing data)**
- **Distributed Denial of Service (DDoS) attacks**
- **Spying via software that tracks activity or keystrokes**
- **Hacking through remote access to your network**
- **Technical debt – old technologies and out-of-date systems give attackers easy entry**

With the pandemic transforming the enterprise into a remote-first work environment, the last bullet is particularly salient today. The rise of work-from-home (WFH) employees, videoconferencing, and virtual private networks (VPNs) for more sophisticated organizations, has expanded the attack surface exponentially. Now, every remote employee device, home router, and WiFi connection subject organizations to their own unique security vulnerabilities, compounding cyber-risks for organizations.

This is especially true considering that 71 percent of respondents in NTEN's 2018 "State of Nonprofit

[8] https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html
[9] https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf

Cybersecurity" report allow their staff to use their personal devices to access organizational emails and business files[10]. Also, according to a recent survey report from cybersecurity firm Malwarebytes, 57 percent of some 200 IT managers, directors, and executives at companies across the U.S. said their use of "remote tools such as Zoom, Microsoft Teams, and Google Hangouts to communicate across the organization had increased significantly" during the pandemic [11].

Malwarebytes found similar "boosts for instant communication/messaging tools like Slack (34.7 percent), cloud storage solutions to manage data securely (33.2 percent), and VPN services to keep communications locked down (26.7 percent)[8]".

This growing attack surface is compounded by the fact that over 59 percent of participants in NTEN's 2018 survey said that they don't provide cybersecurity training to their staff on a regular basis9. Furthermore, only 19.2 percent of NTEN's survey respondents said they offer annual cybersecurity training to their staff. Thus, it's safe to say that nonprofit personnel are generally uninformed about cyber-risk.

Back on the ransomware front, the heightened use of corporate VPNs is of particular concern. In 2020, VPNs have become the fastest-growing ransomware intrusion vector, according to a report from cybersecurity firm SenseCy.[12] The report identified Citrix network gateways and Pulse Secure VPN servers as being the preferred targets for ransomware attackers.

One threat not cited by NTEN is poor password security. Highlighting this risk is the 2019 hack of People Inc., a human-services agency for people with disabilities and one of New York's largest

[10] https://www.nten.org/wp-content/uploads/2018/11/Cybersecurityreport2018NTEN.pdf
[11] https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf
[12] https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

nonprofits[13]. In this hack, two employee email accounts were compromised by an attacker who was able to gain access to one of them via a weak password, according to ZDNet.

Hacked accounts contained clients' sensitive, personal information. Names, addresses, Social Security numbers, financial data, medical information, health insurance details, and government IDs were compromised and stolen in the breach. ZDNet reported that up to 1,000 People Inc. clients were impacted.

Weak user passwords are also highlighted as a top ransomware attack vector for enterprises via Microsoft's Remote Desktop Protocol (RDP) application, which is "today's top technology for connecting to remote systems[14]," according to ZDNet.

"Today, we have cybercrime groups specialized in scanning the internet for RDP endpoints, and then carrying out brute-force attacks against these systems, in attempts to guess their respective credentials," writes ZDNet.

Regarding the second bullet specified by NTEN, the issue of likelihood, probability of a breach is predicated not just on IT security schemes. The digital hygiene of human users also factors heavily into the audit. Work-from-home further heightens the risk of human error, as other people in an employee's household could potentially and inadvertently compromise a networked device that gives an attacker access into the nonprofit enterprise environment.

So, nonprofits must operate under the assumption that the likelihood of a breach, irrespective of what those odds were before the pandemic, has increased.

On the last NTEN bullet, the consequences of a data breach can put nonprofits out of business. Not only do they risk operational interruption, reputational damage, the loss of donor relationships, and ultimately, business failure, but regulatory enforcement also constitutes a growing threat.

[13] https://www.zdnet.com/article/one-of-new-yorks-largest-nonprofits-suffers-data-breach/
[14] https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/

IV. REGULATORY AWARENESS

Michelle Schaap - Attorney

According to Michelle Schaap, a New Jersey attorney who leads law firm Chiesa, Shahinian, & Giantomasi PC's Privacy & Data Security practice, regulatory risk also needs to be hardwired into enterprise threat models. The first step for nonprofits is to determine the state and federal regulations they are subject to and how exactly the exposure of donors', employees', and business counterparties' data could place them under regulatory scrutiny.

Schapp highlights Europe's GDPR, New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act, and California's Consumer Privacy Act (CCPA) as the primary regulations nonprofits should consider when assessing their cyber-risk exposures.

"GDPR impacts nonprofits here in the US to the extent that they solicit and receive donations from EU residents. To the extent that this data is transferred from the EU to US-based operations, there is an added layer of compliance," said Schaap.

"The law requires businesses to secure informed consent when collecting personal data regarding EU-based individuals or data subjects. Further, once such consent is secured, the data gathered cannot be "repurposed" without further consent from the data subject. Data subjects have specific rights and protections under GDPR, including the right of access and correction, the right of erasure, and the right of transportability," she added.

Closer to home for some nonprofit operators is New York state's SHIELD Act, which was adopted in 2019. The SHIELD Act significantly amended New York's data protection and data breach notification laws, expanding its reach beyond businesses that are operating in New York, and imposing new requirements on persons and businesses in possession of New York residents' private data. This law applies to any business that has the personal information of any NY resident, requiring those businesses to adopt proactive measures to safeguard that personal information (PI).

“As for the Blackbaud breach, the NY SHIELD Act requires businesses that entrust PI of NY residents to third party vendors to vet those vendors to confirm they, too, have proactive measures in place to secure PI of NY residents. Also notable is that the law expanded the definition of a “breach” to include “mere” unauthorized access, and not unauthorized, actual acquisition of that PI,” said Schaap.

Regarding the types of proactive measures mandated by SHIELD, the law requires persons or businesses that have New York residents’ PI to institute “reasonable safeguards” to protect that information. Reasonable safeguards generally involve the person or business instituting a “data security program” that implements administrative, technical, and physical safeguards to protect the data.

“While the amendments to the breach notification law have not created a private cause of action, leaving enforcement in the hands of the Attorney General, the fines for failure to provide timely notice of a breach are at least two times those imposed under the prior law,” cautioned Schaap.

Another regulatory regime to prioritize is California’s. The CCPA generally does not apply to nonprofit organizations. However, if the organization is the philanthropic arm of a for-profit enterprise, then it falls under CCPA oversight.

Schaap said, “this law offers to California residents protections and rights similar to those afforded to EU residents under GDPR. Unlike the NY SHIELD Act, CCPA has created a private cause of action for individuals if their data is breached and the organization at issue did not adopt ‘reasonable’ measures to prevent the compromise. But unlike SHIELD, the CCPA does not outline what a reasonable program would entail.”

Schaap also cited the California attorney general’s guidance, which recommends that firms encrypt user PI, redact data, limits access to data, and minimizes collection and storage of data, as a means for businesses to mitigate their legal liabilities.

Finally, there is the issue of health data, which is regulated at the federal level by the Health Insurance Portability and Accountability Act. Schaap said that “many companies frequently misuse or misconstrue” HIPAA.

“HIPAA applies to any ‘covered entity’ and to business associates like those involved in billing for healthcare services. The fact that a company may collect, and store health information does not mean that the company is subject to HIPAA. However, if indeed the company is covered, the company will need to comply with the mandates of HIPAA. Like the SHIELD Act, HIPAA does in fact outline what affirmative measures an appropriate program would entail.”

Nonprofits should also be aware that over 30 states have some proactive legislation in place requiring ‘reasonable’ measures to be adopted by any company that collects, stores, processes, transfers, and deletes PI, noted Schaap. “Even in jurisdictions that do not have proactive legislations, some courts have found, under common law, liability for failure to proactively protect personal information from the foreseeable risk of a data compromise,” she said.

Many jurisdictions also have legislation regarding the requirement to securely destroy records that contain personal information. Additionally, all 50 states have data breach notification laws. “Failure to give timely notice can result in significant fines. But the cost of notification can be significant, depending on the number of impacted individuals,” said Schaap.

V. INCIDENT RESPONSE PLAN

After the known universe of threats has been modeled, nonprofits need to formulate an incident-response plan that they can deploy to mitigate the impact of a data breach when it is discovered.

As such, every nonprofit needs to have a written guide that outlines all of the steps the organization needs to take to remediate the problem. NTEN highlights the following items as integral to this response plan[6]:

- **What mechanisms are in place to detect a security incident?**
- **Who will document the events leading up to and immediately following when the breach was discovered?**
- **Who will lead the response if a breach occurs?**
- **Who will be part of the response team?**
- **How will you respond to various scenarios?**
- **How will your response team communicate with the rest of the organization?**
- **How will your organization recover files or repair systems?**
- **How will your organization communicate with your constituents (if necessary)?**

It makes sense for nonprofits to model their response plans based off of the highest probability scenarios like ransomware and the unintended exposure of donor financial or health records, for example. This reference guide can help keep the organization on the same page when a crisis hits and delineate a clear continuity plan for breaches that seem increasingly inevitable.

Also, key to this incident plan, is the designation of a point person to oversee the response and communicate with relevant counterparties, whether it be IT contractors, or law enforcement investigators, legal counsel, or affected donors themselves. Smaller nonprofits will likely not have the budget to employ a chief information security officer (CISO), but whoever is tasked with monitoring general IT issues, is the logical choice to run point on incident response and remediation.

In the event of a breach, however, it's crucial to clear all external communications with legal counsel first, as miscommunication poses an additional risk in the event any cyber-malfunctions escalate into litigation or regulatory issues.

VI. FITTING CYBERSECURITY INTO TIGHT NONPROFIT BUDGETS

Lacking the robust budgets to employ CISOs or to capitalize the kinds of cybersecurity programs commonly found in larger not for profit organizations, smaller nonprofits are at an inherent disadvantage when it comes to managing risk in the zero-trust era of digital defense.

Cybersecurity is no longer defined by the old perimeter-defense model, where organizations trusted everyone within their networks by default and assumed that firewalls and other barriers could keep adversaries out. Now, enterprises must assume the enemy is already inside. Hence, the zero-trust moniker.

Zero-trust models are thus designed to continuously oversee the IT environment in terms of risk mitigation. According to Cloudflare, zero-trust IT "requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter."[15]

But this exhaustive approach to mitigating cyber-risk can drain precious IT spend, which is generally allocated towards hardware, software, and subscriptions and services. According to consultancy Accenture's 2020 "Annual State of Cyber Resilience" survey, 4644 executives reported that cybersecurity spend comprised 10.9 percent of their IT budgets on average [16].

As a general rule of thumb, organizations should be spending between 7 percent and 10 percent of their annual IT budget on security, advises Frank Dickson, program vice president, cybersecurity products, at International Data Corp. (IDC)[17]. But commercial security solutions aren't tailored to the specific needs of nonprofit organizations. While nonprofits perform business functions similar to private firms, they also have nuances that make their risks unique.

If budget is especially tight, the Small Business Administration advises nonprofits to tap government funding options available to them via the "Access Financing" Wizard from Business USA . [18]Also, certain private nonprofit (PNP) organizations are eligible to apply for pandemic funding via the Federal Emergency Management Agency's Public Assistance program [19]. Lastly, there still may be CARES Act financing options for nonprofits with less than 500 employees.

With the right cybersecurity compliance adviser, nonprofits of all sizes can implement the four pillars of cyber-risk management into their operations and safeguard their donor networks, without breaking the bank. To this end, Partners in Regulatory Compliance, one of New York's leading cybersecurity advisory firms for nonprofits and private sector entities, is here to help.

[15] https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/
[16] https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf
[17] https://www.csoonline.com/article/3432138/how-much-should-you-spend-on-security.html
[18] https://www.sba.gov/category/types-businesses/non-profit-organization
[19] ttps://www.fema.gov/fact-sheet/coronavirus-covid-19-pandemic-private-nonprofit-organizations

Partners in Regulatory Compliance (PIRC) provides an array of cybersecurity services including policy management, risk assessments, employee training, and regulatory compliance assistance to nonprofit organizations in New York, New Jersey, and Connecticut. PIRC is a cybersecurity consultancy that provides innovative answers to the growing, complex need for cybersecurity in nonprofit organizations facing strict regulatory compliance controls. By addressing the full range of digital and human threats to create a compliant, secure environment, PIRC helps nonprofit managers and leaders meet their professional, ethical, and legal commitments to protect the sensitive data they work with and store on behalf of their clients and donors.

Learn more at piregcompliance.com and please feel free to contact us at (646) 863-9050 or info@piregcompliance.com.