MAXXSURE
CYBER RISK MANAGEMENT

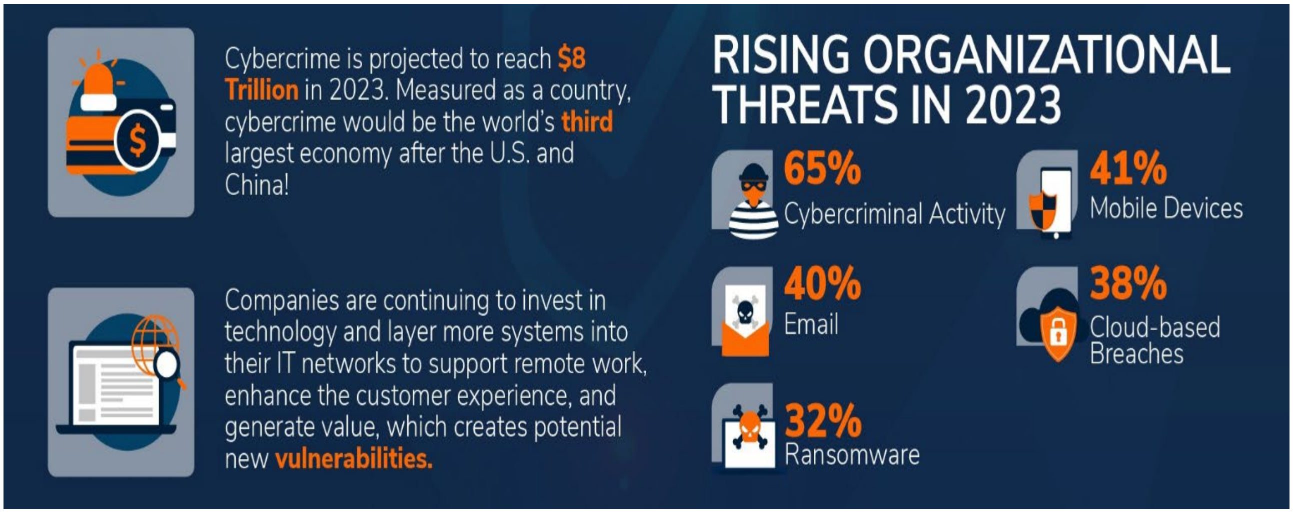
Cyber Risk Management for Non-Profit Leaders

What You can do Now to Protect Your Organization

Chris Burrow and Kevin Hall

April 16, 2023

Global events ranging from the war in Ukraine, hyperinflation, climate change, predictions of a possible economic recession, and cyber threats are continuing to make headline news in 2023. Cyber incidents constitute one of the most immediate threats to organizations large and small, particularly given the costs of paying ransoms, business interruption, remediation, reputational damage, and potential litigation that can follow such breaches.



Cybercrime is projected to reach **$8 Trillion** in 2023. Measured as a country, cybercrime would be the world's **third** largest economy after the U.S. and China!

Companies are continuing to invest in technology and layer more systems into their IT networks to support remote work, enhance the customer experience, and generate value, which creates potential new **vulnerabilities.**

RISING ORGANIZATIONAL THREATS IN 2023

65% Cybercriminal Activity

41% Mobile Devices

40% Email

38% Cloud-based Breaches

32% Ransomware

Non-profit organizations have become a prime target for cyber criminals. This is partly due to the private information many maintain, including data about individuals who are often vulnerable and at-risk, like low-income families, children, the infirm, and the elderly. "Non-profits often don't have the financial resources of for-profit companies, so they are especially vulnerable to cyberattacks. Non-profits also collect sensitive information, such as social security numbers that hackers can use for identity theft," according to a recent article in Forbes (1).

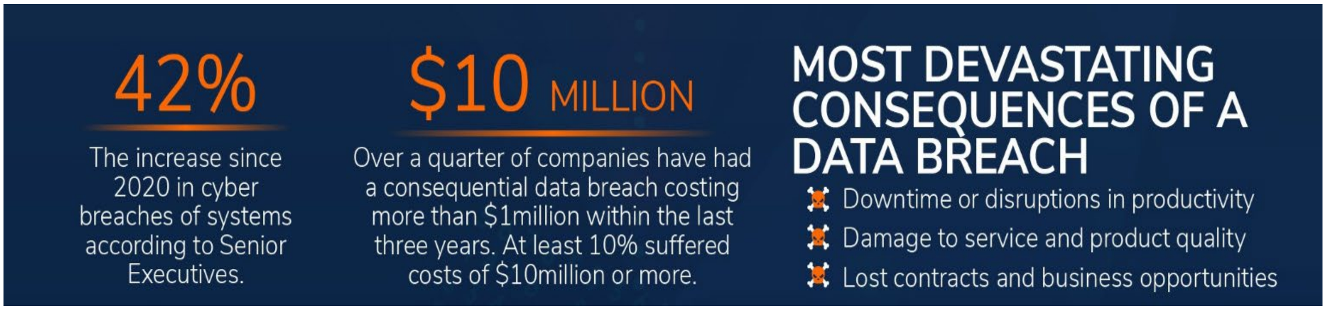
In this article, we examine the cyber challenges unique to non-profit organizations and provide recommendations as to what actions non-profits can take to protect their operations. Fortunately, there are a number of actions, steps, and measures that organizations can implement to help reduce the chance of a crippling cyber breach.

The Unique Challenges for Non-Profit Leaders

Non-profits are confronting a range of risks related to cybersecurity. In the case of non-profits, risks can impact their ability to serve their mission and can lead to civil and/or criminal penalties, according to Forbes. "Non-profits need to protect the privacy of their donors by ensuring that donor information is not disclosed in ways that are not authorized by law. A data breach or other cybersecurity incident that results in the disclosure of sensitive information could damage the organization's reputation, impacting future fundraising and other activities."

Non-profits face a range of threats as outlined in the Forbes study, including:

- ***Data breaches from third-party vendors.*** Non-profits often rely on third-party vendors to store sensitive information, such as donor data, medical records, and Personally Identifiable Information (PII) for fundraising. If a third-party vendor is breached, sensitive data stored there is also at risk of being stolen.
- ***Email phishing schemes***. Email phishing is a form of social engineering intended to trick the recipient into giving up sensitive information, such as their username and password or bank account information.
- ***Data breaches from employees.*** Many data breaches occur due to negligence or malice on the part of an employee, resulting in the theft of sensitive information.
- ***Malicious software (malware).*** Viruses and other malicious software can infect computers or mobile devices connected to the network, putting sensitive information at risk.
- ***Ransomware.*** A form of malware that encrypts data on an infected computer or device and demands payment for the decryption key.
- ***Natural Disasters.*** Storms, floods, and other natural disasters can create a power outage that knocks out internet connectivity or result in physical damage to the building that affects the network.



42%

The increase since 2020 in cyber breaches of systems according to Senior Executives.

$10 MILLION

Over a quarter of companies have had a consequential data breach costing more than $1million within the last three years. At least 10% suffered costs of $10million or more.

MOST DEVASTATING CONSEQUENCES OF A DATA BREACH

- Downtime or disruptions in productivity
- Damage to service and product quality
- Lost contracts and business opportunities

Recommendations for Non-Profit Leaders

Given the above-mentioned threats, what should non-profit leaders do to reduce cyber risk exposure in their organizations? The following are some specific action steps that can be taken and have proven to be effective in attaining cyber risk resilience.

1. **Maintain A Broader Focus on Cyber Risk Quantification Within Organizations**

Organizations which have maintained successful cyber risk practices first define the scope of their risk exposure and quantify that level of risk. This allows organizations to establish their cyber risk management objectives. These organizations assume a risk-based approach which focuses on the most important assets and the biggest, most probable threats.

Quantifying an organization's cyber risk is key to making informed decisions about addressing - and reducing - significant risk and developing a strategy to manage that risk on an on-going basis. It is essential to share this strategy with the entire leadership team including the CEO, CFO, legal counsel, and board.

Non-profit leaders should work as a team and demand a holistic and objective examination of both their internal and external threat environments so they can properly quantify their organization's cyber risk. The resulting business metrics and supplemental insights will empower leaders to make the best cyber risk management decisions for their organizations, thereby demonstrating due diligence and minimizing their potential financial loss.

Without a concrete quantification of cyber risk in financial terms, leadership will struggle to allocate funding that properly safeguards their assets. An organization should adopt a solution that provides clarity of their cyber risk exposure and the financial impacts so the best management decisions can be made.

2. Increase Engagement by Leadership Team

In today's high-risk environment, addressing cyber risk at the leadership level is of utmost importance. The leadership team must recognize cyber risk as a business problem, not just an IT problem. Cyberattacks jeopardize business assets and, by extension, the financial livelihood of the entire enterprise.

C-Suites are taking bolder approaches to lead in the area of cyber risk management, according to PwC's Global Digital Trust Insights 2023 (2). Corporate leaders are beginning to "step out of their independent cyber-specialist role and into one of partnering with not just a few executives, but the entire C-Suite. These collaborations have never been more critical."

CEOs who have suffered breaches within their organizations are particularly determined to accelerate their management of cyber risk. They want more information to help them make informed decisions to oversee their organization's cyber risk exposure. And they want to report more fully and in more detail to their boards and constituents as to exactly what measures are being taken, according to the PwC report.

Key findings of the PwC study include the following:

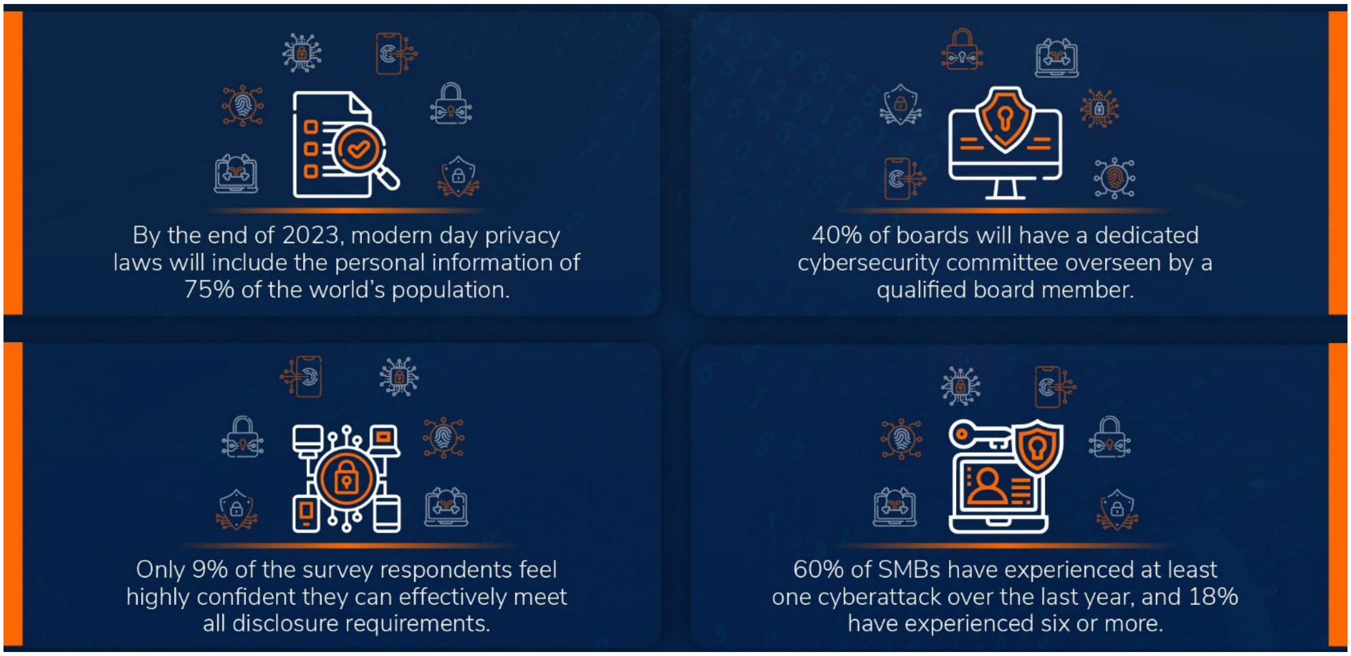
- Forty-two percent of senior executives say cyber breaches of their systems have increased since 2020.
- More than a quarter have had a consequential data breach in the past three years costing more than $1 million. At least 10% have suffered costs of $10 million or more.
- To CFOs, the most devastating consequences when a breach occurred were:
    - ✓ Downtime or disruptions in productivity
    - ✓ Damage to service and product quality
    - ✓ Lost contracts and business opportunities

3. Initiate More Rigorous Board Oversight

As the cyber threat landscape continues to evolve and become more sophisticated, "the role of the Board of directors in cyber risk oversight is becoming increasingly important," according to Deloitte (3). As organizations focus on continued growth while maintaining customer trust, "the Board can help position Cyber as a strategic enabler to foster stronger relationships among customers, vendors, employees, and shareholders."

Due to these factors, security and risk management have become a priority for board-level oversight within many organizations. Security breaches are not only becoming more common but are becoming more complex as well. As a result, new laws are being passed to protect consumers and companies.

Most organizations focus on cyber protection rather than cyber resilience, according to a recent article in the *Harvard Business Review*. "Resiliency is more than just protection: it's a plan for recovery and business continuation. Being resilient means that you've done as much as you can to make sure you can continue to operate when an incident occurs" (4). Based on Harvard supported research, most board members believe it's not just a matter of if, but when their company will experience a cyber event. Cybersecurity is a continuously changing and moving target. The more often the board is exposed to the cyber-environment of their organization, the more comfortable and more expert they become."



By the end of 2023, modern day privacy laws will include the personal information of 75% of the world's population.

40% of boards will have a dedicated cybersecurity committee overseen by a qualified board member.

Only 9% of the survey respondents feel highly confident they can effectively meet all disclosure requirements.

60% of SMBs have experienced at least one cyberattack over the last year, and 18% have experienced six or more.

4. Adapt to a More Complex Regulatory Environment

By the end of 2023, modern day privacy laws will apply to the personal information of 75% of the world's population, according to predictions developed for 2023-2025 by Gartner (5). New regulatory mandates are emerging rapidly. Meanwhile, the US Securities and Exchange Commission is considering requiring publicly held companies to disclose their cyber risk management, strategy, governance, and "material" cyber incidents. Specifically, where pertinent to board oversight, publicly traded companies will be required to disclose:

- Whether the entire board, a specific board member, or a board committee is responsible for the oversight of cyber risks.
- The processes by which the board is informed about cyber risks, and the frequency of its discussions regarding cyber risks.
- Whether and how the board or specified board committee considers cyber risks as part of its business strategy, risk management, and financial oversight.

The scope and reach of these regulations are forcing corporate leaders to manage multiple data protection laws in multiple geographic regions. On the regulatory front, only 9% of the PwC survey respondents feel highly confident they can effectively meet all disclosure requirements – even as pressure mounts from regulators to report cyber incidents.

Also, customers are increasingly demanding information on what kinds of personal data is being collected from them, with what groups that data is being shared, and how it is being used. "This means that you need to focus on automation of your data privacy management system. As for how to do this, basically using GDPR, you can standardize security operations and then tailor it to individual jurisdictions," according to the study.

5. **Evaluate and Track Third Party Risk**

Third parties include external actors, such as people in a company's supply chain who are participating in providing goods and/or services. They include subcontractors, suppliers, and vendors. These parties can expose an organization's confidential data such as intellectual property, financial data, and customer records if proper measures are not in place. Every organization should monitor and track the cyber risk management policies of their third-party vendors just as they would their own company.

Case Study: Third Party Cyber Risk and the Blackbaud Breach

Blackbaud is a South Carolina – based software company and one of the world's largest providers of educational administration, fundraising, and financial management software for non-profit organizations. A major breach that occurred in 2020 served as a wakeup call to thousands of organizations, many of which previously assumed that non-profits were somewhat off the target list of hackers and other bad actors. Hundreds of customers that used Blackbaud's fundraising platform learned that their data was breached and held hostage in an elaborate ransomware attack. The breach was named the "largest health care breach of 2020."

Non-profit organizations that were affected by the breach not only included healthcare organizations, but colleges and universities, churches, food banks, foundations, and many others. Prominent organizations breached through use of the software included the George W. Bush Presidential Center, the Hockaday School, the Human Rights Watch, Middlebury College, the Rhode Island School of Design, and many others. Blackbaud states that it has 45,000 non-profit and governmental customers in 100 countries. According to the SEC, the cyberattack affected more than 13,000 Blackbaud customers.

The ransomware attack was discovered in May of 2020, but Blackbaud did not disclose the breach until the following July. In a statement from the SEC, "Blackbaud failed to disclose the full impact of a ransomware attack despite its personnel learning that its earlier public statements about the attack were erroneous." Blackbaud was required to cease and desist from committing future violations and paid a $3 million civil penalty.

6. **Adapt to a Challenging Cyber Insurance Marketplace**

The cyber insurance marketplace is a complex and confusing sector in the insurance industry that is still in its infancy. Cyber insurance is evolving rapidly in terms of its availability, pricing, limits, and exclusions. The cyber insurance marketplace is also highly volatile. According to Tom Johansmeyer, writing in the *Harvard Business Review*, "while more attacks could stimulate demand, they also create a supply problem, making insurers warier of providing coverage and reinsurers less interested in backing cyber liabilities. On top of that, the lack of historical loss data adds another layer of unpredictability for all involved" (6).

According to a recent report by Gallagher, "carriers have been under pressure due to the increasing frequency and severity of cyber claims and a rapidly expanding regulatory environment at the state, federal, and international levels" (7). As a result, there will likely be a reduction of capacity in the market, which will likely continue to increase pricing. Some industries are already seeing significantly higher premiums and a "pulling back" from high-risk industries all together.

Cyber risk insurers are requiring much more diligence on the part of applicants and existing policy holders including maintaining a comprehensive cyber risk management plan, a cyber risk registry, monitoring cyber risk exposure, and protecting themselves from third party risk.

7. **Engage in Ongoing Cyber Risk Management**

Organizational leaders should work to ensure cyber risk quantification is performed on a continuous basis to gauge progress toward program goals. Cyber risk management must be treated as an ongoing process because cyber risk is constant, ever-present, and continuously evolving. Conducting regular audits, making cyber a strategic priority, and performing cyber risk assessments are some of the most important steps organizations can take to prepare for cyberattacks.

Summary

In 2023, reputational consequences from cyber incidents will be bigger than ever before. Regulatory requirements for safeguarding data privacy are now agnostic to both industry and company size. Third party cyber risk from your supply chain will continue to increase both as the root cause of cyber incidents as well as increase the financial, disruption, and reputational impact on your organization.
The biggest cyber risk in 2023? How you choose to identify and quantify cyber risks.

Most important cyber risk decision in 2023*?* How you choose to manage cyber risks, on a continuous basis, and aligned with the dynamics of and innovation pace within the cybercrime industry.

Most preventive effort to protect company reputation and valuation? Establish a robust cyber risk registry to defend company and fiduciary leadership against future negligence claims.

References Cited

(1) Forbes, The Necessity of Cybersecurity in the Nonprofit Sector by John Giordini, Forbes Technology Council, November 8, 2022.

(2) "A C-suite united on cyber-ready futures," Findings from the 2023 Global Digital Trust Insights Survey, PwC

(3) Deloitte Perspectives: *Sharpening the Board's Role in Cyber Risk Oversight,* by Deborah DeHass, Vice Chair, Deloitte, and Ed Powers, Principal, Deloitte, January, 2023.

(4) Harvard Business Review - IT Security Management, *Is Your Board Prepared for New Cybersecurity Regulations?* By Dr. Keri Pearlson and Chris Hetner, November 11, 2022

(5) Gartner/Gartner IT Symposium 2021/ Sam Olyaei- *Gartner's 8 Cybersecurity Predictions for 2023-2025,* Feb 16, 2022, Krontech

(6) Harvard Business Review, Risk Management, *"The Cyber insurance Industry Has a Big Problem,"* by Tom Johansmeyer, January 11, 2021.

(7) Arthur Gallagher and Company, Cyber Liability Practice, *Cyber Risk Exposures and Solutions,* by Adam Cottini, Managing Director, Cyber Liability Practice, January, 2023.

About the Authors

Chris Burrow is a Partner and Senior Strategic Advisor at Maxxsure Cyber Risk Management based in Addison, Texas. Chris has served in CEO, CFO, COO, and board positions in both for-profit and non-profit organizations for over 30 years. Those include organizations in the real estate services and advisory sectors as well as educational institutions and foundations. Chris enjoys cycling, golf, mountain climbing, and business writing in his spare time.

chris.burrow@maxxsure.com

Kevin Hall is President of the Grant Halliburton Foundation in Dallas. He previously served as Chief Operating Officer of the foundation. Prior to Grant Halliburton, Kevin was a leader in the marketing and advertising industry and served in an Account Management position with Temerlin McClain for 15 years. In that capacity, Kevin was responsible for leading the strategic planning and execution of local, regional, and national advertising campaigns on behalf of major national companies including Zale Corporation, Greyhound Lines, Bank of America, and others.

khall@granthalliburton.com

About Maxxsure

Maxxsure is a cyber risk quantification, management, and advisory firm based in Addison, Texas. The firm’s services and proprietary management platform enable clients to confidently identify, quantify and manage cyber risk.
The firm’s customers include global industry leaders in commercial real estate services and investments, financial services, law, ratings, gaming, wealth management, telecommunications, and data management, to name a few. Customers range in size from $25 million to $25 billion in annual revenue.

Maxxsure was founded in 2016 with the mission of developing the best-in-class cyber risk quantification and management solution that takes a truly holistic survey of all internal and external influencing factors over the cyber risk posture of an organization.

With Maxxsure, organizations have continuous line of sight into their cyber risk, allowing them to access up-to-date data to make adaptations to their cyber risk management strategies as their needs and environments change. The company provides a platform for executive management, leveraging proprietary technology that:

- *Identifies, measures, and scores an organization’s cyber risks.*
- *Uncovers hidden risks in a business model, including vendors/supply chain.*
- *Illustrates how prepared/resilient an organization is against a cyber event.*
- *Estimates potential financial loss of future events.*

MAXXSURE

www.maxxsure.com

CORPORATE OFFICE:
4570 Westgrove Drive Suite 235
Addison, Texas 75001 USA