4 CYBERSECURITY MYTHS

that are

Sabotaging Your Organization

†This is not a CPA firm.
*Assurance, attest, and audit services provided by Carr, Riggs & Ingram, L.L.C.

CRI CARR RIGGS & INGRAM®

criadv.com

TABLE OF CONTENTS

When it comes to cybersecurity, a number of myths persist among small businesses and nonprofit organizations. These blind spots can put your organization at higher risk.

In this e-book, we'll examine four cybersecurity myths, how they could be making your organization less secure, and how to overcome these misconceptions to build a strong cybersecurity culture.

MYTH

"Cybersecurity is an IT problem. It's not my problem."

If we asked you who is responsible for information security at your organization, who would you say? Would you say the IT manager? The entire IT department? An information security officer?

Many organizations share this sentiment — that the responsibility for cybersecurity is held by a few people. But let's explore this misconception and why cybersecurity is actually the responsibility of every individual at an organization.

Cybersecurity is a business risk.

Cybersecurity is not just an IT risk. If an incident occurs, an organization may experience fines, penalties, and legal fees. Organizations can also experience reputation damage as clients, donors, and other constituents lose faith in the organization's ability to protect their sensitive information and donations.

These types of threats are damaging to the organization as a whole, not just the IT department. Organizations often struggle to recover from the short-term and long-term financial impact of a breach. And that affects all employees, not just the IT staff.

Response to breaches includes more than just the IT department.

When a breach occurs, IT staff are undoubtedly involved. However, appropriate breach response does not just include technical employees. Your public relations and marketing staff should be involved to ensure your constituents and the media are updated appropriately. Legal counsel generally must be consulted to ensure all applicable laws and regulations are considered. Human resources, security, operations personnel, and other levels of management may also get involved, depending on the type of incident.

An end user can prove to be the weak link.

Good employees make mistakes all the time. Even if your technical department puts every possible control in place, there will always be that one staff member who is in a rush, improperly trained, or just makes a mistake. These people will click on a phishing link that installs malware or will improperly authenticate a request and give out sensitive data.

Cybersecurity is the responsibility of your entire user base, and this responsibility needs to be communicated, starting from the top down.

MYTH

"We've never had a breach. Our IT department must be keeping us secure."

Have you heard this sentiment from the C-level of your organization? Do you find yourself saying this in management or budget meetings as a reason why additional IT or information security expenses are not justified? Have you heard this as a justification for why your organization doesn't need to hire a separate information security officer?

You're not alone. Many organizations view IT and information security as one and the same. They assume that because IT is doing a great job, the organization must be secure and have little risk of being affected by malware, hacking, phishing, breaches, or other incidents.

There are two primary reasons why this is a myth.

IT and information security are different.

IT and information security are two very different functions, and relying on the IT function alone to secure your organization would be a disservice to you, your clients and other constituents, and your mission. While IT and information security often work in conjunction with each other, they have different goals, priorities, and required skill sets.

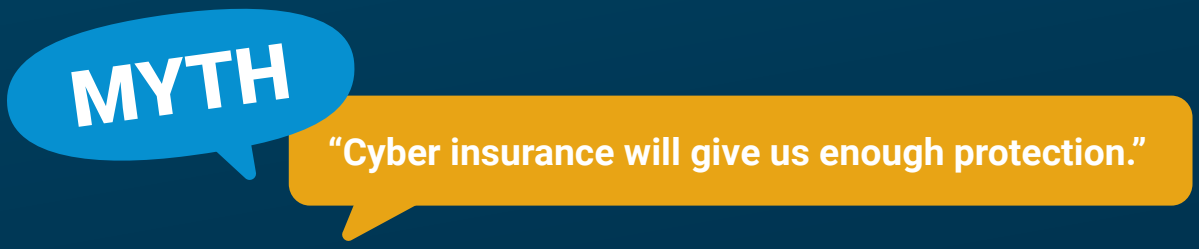
IT is needs-focused and has the ultimate goal of helping the organization with ongoing maintenance and support of the technology, infrastructure, and systems. The IT department resolves end-user issues, recommends enhancements to infrastructure, and works to increase the effectiveness and efficiency of existing technology. IT staff must have very specific technical knowledge and competencies related to the hardware, software, and network components actually used within the organization.

The primary goal of the information security department staff is to assess risks, design controls to mitigate those risks, and establish monitoring procedures to identify deviations. Information security staff members must maintain competencies related to risk evaluation and mitigation. While information security staff must have a basic understanding of various forms of technology, the role typically does not require the same level of technical detail and hardware-specific knowledge that IT does.

Security often takes a back seat.

IT and information security are generally not income-producing departments, and these two functions often share budgets and resources. When budgets get tight, the needs of IT — supporting the infrastructure and ensuring technology runs as intended — often take precedence over the security-related needs, tools, and processes of the information security department.

It's imperative for organizations to understand how IT and information security work together, the differences between them, and how to empower them to flourish in tandem. Efficiency and effectiveness do not automatically mean security. And while your IT department may perform at a high level and staff may experience ease and efficiency in their day-to-day work, the reality is that the solutions may not be secured adequately if staffing and budgets are not allocated sufficiently between IT and information security.



With the continued headlines about cyber breaches and incidents, **cyber insurance** has become a buzzed-about topic. Debates about whether organizations should invest in this type of insurance continue to occur in management and board meetings. And if you have not had these discussions yet, you should!

However, it's a myth that cyber insurance (also called cyber risk insurance or cyber liability insurance coverage) is a cure-all. Let's evaluate the biggest pitfalls with believing cyber insurance is the panacea to the threats that continue to plague our cyber world.

Sometimes insurance doesn't cover what you think it does.

The biggest issue is that organizations often don't have a handle on what their insurance policies do and do not cover. Cyber insurance is a vague term, and there are many layers and facets.

It's imperative to take the extra time to delve into the coverage and gain a comprehensive understanding of the policy. Ask the following questions:

- **What types of incidents are covered?** There are so many types of cyber incidents (e.g., distributed denial-of-service (DDoS) attacks, ransomware and other forms of malware, electronic theft, deletion or corruption of data), and policies may stipulate what types of incidents are covered.
- **What type of coverage is included?** Consider coverage of legal fees and penalties, notification to affected parties, forensics or incident investigation services, incident response coverage, and loss of income due to disruption of operations.
- **How is a claim made?** What minimum requirements must you meet to make a claim? What documentation is required to make a claim? Some policies may require certain data and evidence to submit a claim. If you can't provide this, you may not be able to make a claim.

You often need to meet baseline controls to make a claim.

To obtain insurance, organizations are often required to complete an extensive questionnaire that asks about controls and policies. Many cyber insurance policies have stipulations for baseline controls that need to be met. Your policy may require a documented risk analysis of controls and firewall and other perimeter security protections, or an annual IT/information security audit.

If your organization doesn't have the stipulated baseline controls in place, you run the risk of your claims being denied. Many organizations get cyber insurance without reading the fine print, or they attest to controls they either don't understand or don't have in place. When the time comes to make a claim, if they can't prove they had these controls, they may be out of luck.

An adequate policy one year may be insufficient the next.

If you do purchase cyber insurance, you need to revisit the policy annually. First, threats and risks are constantly evolving and changing. Does your policy still cover the areas that are applicable to you? If not, you may need to work with your broker to make adjustments.

Second, are you still meeting the stipulations within the policy? As noted above, many policies require baseline controls in order to file a claim. Many organizations make enhancements to their control framework throughout the year as new technology and enhancements become available. This is great — unless you forget to come back to the policy stipulations.

If you decommission an existing layer of control for another more robust option, check to see whether you have invalidated your ability to make a claim by doing away with a required control as defined by the policy.

Cyber insurance doesn't cover a loss of trust in your organization.

Keep in mind that while a cyber insurance policy may help you recoup financial losses related to penalties, fines, and disruptions of operations, no insurance policy can cover future lost revenue or monetary contributions that donors haven't made yet.

If you have a cyber issue that results in a breach of sensitive donor information or loss of funds, donors may lose confidence that your organization can protect their information.

Our goal is not to discourage you from getting cyber insurance. It is a great tool to have and can be a critical component of your information security strategy. However, it should not be the only layer of control you implement. Instead, combine cyber insurance with regular **cybersecurity assessments**, a designated information security officer to oversee this critical area, a layered control framework, and a partnership with legal counsel that can aid you in defending cyber claims.

MYTH

"The cost of investing in security is too high."

It's a fact that the average organization's information security function is not income-producing. And you may find yourself struggling to justify information security-related expenses — whether for a new tool to provide enhanced monitoring, the salary for a dedicated information security officer, or expenses for an IT/information security audit.

However, while security requires financial resources, it's a myth to think that the cost of security is too high to justify. Let's investigate why this myth is unfounded.

The risk of a breach is growing.

With the use of connected devices, which will continue to increase, and a rise in remote work, the risk of a breach is only growing. For most organizations, control failures, incidents, breaches, phishing attacks, and other cybersecurity issues are not a matter of "if" but "when." And "saving" money by neglecting to invest in security now can cause significant financial loss in the future.

The average cost of a breach is high.

There is so much data within most organizations, and the cost of a breach can quickly reach a significant level. The **IBM Cost of a Data Breach Report 2025** found that the average total cost of a data breach was $4.44 million per breach globally. The country with the highest average cost was the United States, at a whopping $10.22 million per breach, and the healthcare industry had the highest average cost at $7.42 million per breach.

For small organizations, the absolute numbers are much smaller, but the impact can be devastating. When considering how your organization could be affected, an important takeaway from this study is the average cost per lost record. In IBM's 2025 report, the average cost per lost record of employee personally identifiable information (PII) was $168, and the average cost for lost customer PII was $160. While this may not seem like a lot, consider how many records your organization has, such as records for employees, donors, patients, members, clients, and other constituents. With a breach of 1,000 records, the cost could add up to $160,000 or more.

Ask yourself: How many records does our organization have? Would we be able to recover if a breach affected these records?

The cost of a breach can be reduced with controls.

Breach costs are not one-time costs. In fact, most organizations are affected multiple years after the initial breach. However, implementing mitigating safeguards can lower overall breach costs. And organizations that identify breaches more quickly experience significantly reduced costs. Therefore, resources you devote now to prevent, detect, and respond to incidents can minimize the short-term and long-term financial impact on your organization.

In addition, many cybersecurity controls can increase the efficiency and effectiveness of existing processes. For example, a centralized monitoring tool may allow your IT staff to more effectively monitor the patch and anti-malware management processes. So while there is an up-front cost to implement that tool, your staff will have added time savings that will allow them to devote their expertise to other critical functions, such as incident identification.

Ask yourself: Does the up-front cost of investing in the tools and resources to empower the cybersecurity of our organization outweigh the risk and cost of a breach?

You can't put a price on your reputation.

The loss of reputation can be a significant cost for organizations. If you have a cyber issue that results in a breach of sensitive donor, client, patient, or employee information, your constituents may lose trust in your organization.

Your constituents may turn to organizations that they feel can better protect their information. Nonprofit donors may look for organizations that are better able to use their donated funds for the mission rather than losing it to hackers. The loss of future revenue streams can have a significant impact on an organization's ability to continue.

Ask yourself: Does the cost of investing in security now outweigh the risk of my organization being unable to complete its mission due to loss of reputation related to a breach?

It cannot be denied that the cost of a breach is high. And unfortunately, many organizations that suffer breaches do not recover and instead close their operations. That's why it's important to view security controls as an investment. With this mindset, you'll likely find that the potential impact of an incident significantly outweighs the up-front cost for preventive, detective, and response controls.

Data breach costs are largely deductible.

No data loss prevention policy is perfect, but a good one will almost always be worth the cost. And fortunately, most of these expenses are tax deductible.

Data loss prevention methods — such as using data theft detection software, regularly reviewing data for inaccuracies, auditing the data environment for risks, purchasing encryption technology, installing more robust hardware, and implementing better network security — are ordinary and necessary business expenses. This means they are deductible for both federal and state income tax purposes

for businesses filing as C corporations, S corporations, or partnerships, and to self-employed persons reporting their business activity on Schedule C.

By the same token, virtually all measures taken to control a breach — including ransom payments — are ordinary and necessary expenses and should be fully deductible. Losses arising from theft are deductible under Internal Revenue Code (IRC) Section 165. (Note that any costs that are covered by insurance are not tax-deductible.)

Ransomware attacks are considered theft by extortion and are therefore deductible. The IRS makes this clear in Revenue Ruling 72-112, when they state that ransom payments qualify as a theft loss deduction as long as the extortion was illegal in the state where it occurred. Although the revenue ruling was in response to a ransom paid in a kidnapping, the ruling is often applied to ransoms paid to recover digital assets or data.

Low-Cost, High-Reward Investments in Cybersecurity

When organizations are facing financial challenges, making investments in cybersecurity often takes a back seat. However, there are low-cost steps you can take to address cybersecurity gaps while facing budget shortfalls.

Become a cybersecurity champion. A culture of security starts at the top levels. Staff must see management taking responsibility for cybersecurity, and this can be established by having standing IT/information security department updates at board meetings.

Establish a cybersecurity training program to ensure staff members understand the threats that are out there and what they can do to help keep your organization secure.

Implement authentication requirements, requiring longer, more complex passwords for critical IT systems and multi-factor authentication for critical and high-risk systems.

Develop an incident response plan that includes input from applicable departments. Conduct tabletop testing (a discussion-based exercise in responding to a hypothetical incident) where these individuals discuss various scenarios and how the plan would be enacted.

LET US HELP

Need help making cybersecurity a priority for your entire organization?

Or tightening up your existing controls?

We can help you put in place a practical strategy.

Contact our cybersecurity advisors with questions or to learn how we can help your organization assess and reduce your cybersecurity risk.