Cybersecurity Essentials for Association and Nonprofit Leaders

The complete guide to protecting your financial and digital assets.

An eBook written by

designDATA
Empowering Your Best Work

What's Inside

Why Associations & Nonprofits Need Cybersecurity Now More Than Ever

Too many organizations wait until they have been affected by cybercrime before they take security seriously. Years ago, one of the most widespread cyberattacks started with a request for bank information from a "friend" who needed help, and it was pretty obvious to spot. However, in recent times with staff operating outside of the physical office more frequently, and with the rise of AI tools, cyberattacks come in different and unsuspected forms.

Due to global challenges, more organizations rely on technology to assist with daily operational processes. Reliance on technology, and the need to provide access any time and anywhere, has ushered in a new age of cybercrime. Public cloud services that provide email, documents and web services are enticing to bad actors and are well-known targets that may only be protected by a simple password. Phishing and social engineering attacks provide cybercriminals with access to email accounts, which are then used as stepping stones to execute password resets on banking websites. Impersonating a coworker via email is easier when employees aren't sitting next to each other.

Cybercriminals are finding new ways to profit off cybercrime through invoice manipulation, ransomware and data breach extortion. Attackers infiltrate systems months prior to making their move, and organizations may not realize their financial assets or data have been stolen until weeks later. The risks posed by cybersecurity threats can lead to significant financial losses, loss of critical systems and data, irreparable damage to an organization's reputation and even bankruptcy.

So, why should you read this book? Our goal is to equip associations and nonprofit leaders to have the right cybersecurity-focused conversations with their IT teams, leadership and staff. This Ebook presents a true story about a cyberattack that happened to a local nonprofit, along with information on the tools and resources that you can use to strengthen your association's security measures.

Over the years, cybercrime has gone through many changes, becoming more advanced and well-organized. However, one thing remains the same: criminals continue to exploit the weakest link in your security for personal gain. That weakest link could be an improperly configured firewall, an overly trusting employee, a lack of Multi-Factor Authentication, or inadequate identity validation procedures for financial transactions. Today, cybersecurity goes well beyond anti-malware and antivirus protection: It involves developing policies, training your staff on security awareness and the implementation of tools that help close the gaps and maintain the confidentiality, integrity, and availability of an organization's data and computer systems.

designDATA

Established in 1979, designDATA is an IT Managed Services Provider operating out of the Washington, DC Metro area. Employing over 100 local IT specialists, we are focused on equipping organizations with scalable solutions that enable teams to do their best work securely. We do this by striving to see the world through our clients' eyes, aligning IT operations with organizational priorities, and ensuring staff have the resources they need to excel. We help you harness the power of IT through 24/7 tech support, data center and cloud services, robust cybersecurity solutions, exceptional end-user training, and enterprise-level consulting services.

CHAPTER 1

The Cybercrime Threat Landscape

The Cybercrime Threat Landscape

Contrary to the decline observed between 2021 and 2022, recent statistics indicate a resurgence in ransomware activities.

A striking 1,900 ransomware attacks were reported in just four countries (the US, Germany, France, and the UK) within a year, as highlighted in Malwarebytes' 2023 State of Ransomware Report. The US bore the brunt of these attacks, shouldering 43% of global ransomware incidents. The report also notes the rise of the CL0P ransomware group, which utilized zero-day vulnerabilities for amplified impact.

READ MORE >

In terms of repercussions, the effects of ransomware on organizations are profound:

> **Around 46% of organizations reported significant loss of revenue following a ransomware attack.**
>
> **A troubling 40% of companies affected by ransomware had to lay off employees.**
>
> **Regardless of the size of attack, more than 80% of people who pay a ransom will be attacked again.**

The third quarter of 2023 set a new record for ransomware with 1420 cases, marking it as the most successful quarter for ransomware ever recorded. The US remained the most targeted country. Surprisingly, large enterprises aren't the only targets; small to medium-sized organizations are also at significant risk. A third of impacted companies had 101-1,000 employees, and nearly 28% had 11 to 100 employees.

Predictions and Precautions for 2024 and Beyond

AI-Driven Cybersecurity Threats: The role of artificial intelligence in cyberattacks is expected to grow, leading to more sophisticated and challenging security breaches. Organizations will need to adapt their defenses to counter these AI-informed attacks.

Increased Adoption of Proactive Security Tools: There will be a greater emphasis on investing in proactive security tools and technologies. These tools include risk-based vulnerability management, attack surface management, and security control validation through penetration testing and breach and attack simulation.

Supply Chain Attacks: The continued rise in supply chain attacks necessitates robust security frameworks. Organizations need to be wary of third-party security vulnerabilities and consider creating security checklists or requiring third-party security evaluations before doing business with any vendor.

Exploit Mapping for Ransomware: Attackers will shift their focus from data extortion to selling exploit and vulnerability information about organizations. This trend highlights the need to continually update security strategies to protect against evolving ransomware tactics.

Identity Verification Technologies: More organizations will adopt identity verification technologies to ensure the authenticity of employees, partners, and members during account onboarding and access requests.

Mitigating Risks

Organizations should continue to develop robust cybersecurity strategies and maintain updated security protocols, anticipating and adapting to the evolving threat landscape.

Conduct regular risk assessments and manage vulnerabilities proactively to identify and mitigate potential security gaps.

Educating staff remains crucial, especially with the rise of AI-driven attacks and increasingly sophisticated social engineering tactics.

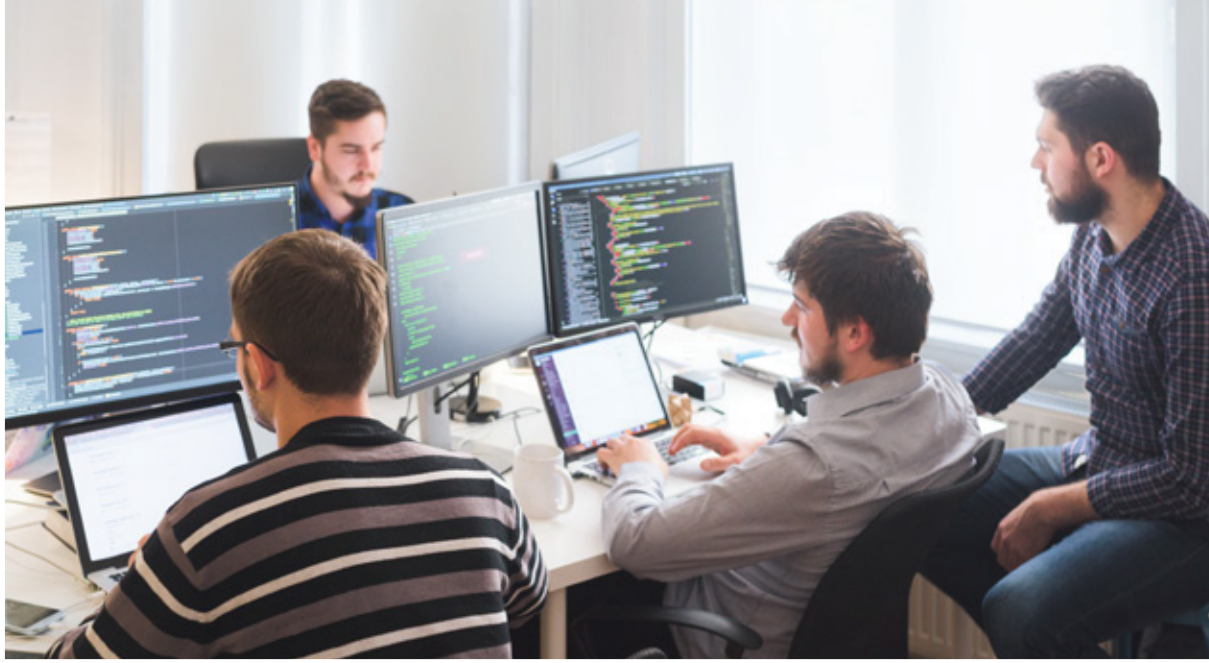
CHAPTER 2

The True Story of a DC-Based Nonprofit That Fell Victim to an In-Depth Cyberattack

The True Story of a DC-Based Nonprofit That Fell Victim to an In-Depth Cyberattack

It was 8:00 p.m., the end of a typical busy weekday. An email came to our team; it was a plea for help from a prospective client we had talked to about security services earlier that day. They had been hacked, didn't have faith in their current IT provider and needed immediate assistance navigating a security breach. Over the next few days, we helped to manage the security event and determine the root cause.

The organization became aware of the situation when they received a call from the bank about suspicious activity. People outside of the organization also reached out about receiving emails from the executive email accounts that looked suspicious. But everything had seemed normal; no one internally had received suspicious emails or fraud alerts. **What was compromised? How was it compromised? How much data did these bad actors have? How long had these criminals had access?**



Our team did a thorough review to uncover the depth of the breach. We determined:

1. The CFO's password to Microsoft 365 had been hacked, and since he was an admin, this provided access to control email for the entire organization.
2. The cybercriminals identified the CFO's bank account, so they reset the password while ensuring the CFO never saw the email.
3. They changed the company's street address within the bank's records, issued three new credit cards to themselves and started putting transactions through them. The bank sent fraud alerts, but the emails were re-routed and never seen by anyone within the company while the hackers confirmed the transactions as legitimate.
4. The attackers reset the password to the master account of their file-sharing service and exfiltrated a copy of all their documents.
5. We determined that they had been in the system for at least 30 days. Unfortunately, the default setting on their Microsoft 365 logs had not been modified, so 30 days of history was all that was available.

These criminals carefully watched and planned how to extract as much information as possible before striking multiple targets simultaneously to increase their chance of success. They were swift, organized and smart, targeting three areas – email, banking and file sharing.

Enter the Experts: How designDATA Acted Fast to Close the Security Gaps

We helped the organization navigate this security incident by doing a full review of their IT environment and cloud service accounts. We locked down all accounts and implemented multifactor authentication (MFA) for all email, banking and file-sharing services. We did a thorough review of their email system. We found six different cases where an unauthorized party had set up rules to divert important emails that would flag concern away from the intended recipient and to the hackers externally.

This customer did not have an incident response plan, so we helped them determine a well-thought-out response to carry them through the breach. We helped them identify the implications outside of IT's scope, such as law enforcement, media relations and staff communication, and pointed them towards organizations with subject matter expertise in those areas. A forensics company performed additional reviews to satisfy their cyber insurance requirements, which enabled them to file a claim to cover their losses.
To this day, the company has never received a ransom note, but the threat remains. These cybercriminals still have all of the company data from their file-sharing accounts and could potentially send a ransom note at any time.

Unfortunately, this organization lacked the proper layers of protection that could have prevented or detected the attack. Since they had nothing in place, the hackers got everything.

The right incident response plan can help mitigate and limit the damage but can't eliminate the risk of having had a data breach in the first place. Throughout this Ebook, we outline **strategies that organizations can implement to reduce an attack's probability and minimize the impact**.

"We had an email breach in the final months with our old vendor. designDATA stepped up the onboarding to accommodate and, even though we weren't their client yet, helped us resolve the breach. The remainder of the transition, including staff training, has been seamless."

~ Chief Operating Officer for Pharmaceutical Association.

READ THE FULL SUCCESS STORY HERE >

CHAPTER 3

Large Organizations Aren't The Only Targets

Large Organizations Aren't The Only Targets

In 2023, the ransomware landscape has seen significant changes, with a staggering 66% of small and medium-sized organizations experiencing ransomware attacks, as reported in Sophos's "The State of Ransomware 2023" report. This marks a notable increase from previous years, underscoring the escalating threat to smaller organizations, including associations and nonprofits.

So, why don't we hear about this more in the news?

A small organization getting hit with a ransomware attack is often not newsworthy in today's atmosphere, and they are under no legal obligation to alert the press. Suppose your association is the victim of a cyberattack. You only need to inform the individuals it has impacted, but you don't need to make a press statement until it reaches a certain threshold of data records; that threshold is usually quite high. It is also embarrassing to admit, and terrible for public relations, so many organizations don't report a security incident unless they have to.

There is a lot of cybersecurity information available, and it can be challenging to navigate through what is critical to consider for your business. However, it is essential to understand some of the myths and facts around cybersecurity so you can ignore the noise, have a discussion with your IT provider and rest easy knowing you are adequately protected and prepared.

CHAPTER 4

Top 10 Cybersecurity Myths

Top 10 Cybersecurity Myths

1 "We're too small to be a target."

The misconception that smaller organizations are not appealing targets for cybercriminals is dangerous. When large enterprises such as LastPass and Microsoft report cyberattacks, it creates a false sense of security for smaller companies. They may think they are too small to be targeted or that it won't happen to them. They might not have a large budget to spend on cybersecurity; perhaps they blindly trust that their IT team is appropriately protecting them, or they don't want to burden staff with additional policies and procedures. The reality is, **there are a lot of ways to protect your organization from cybercrime without breaking the bank.** In fact, there are policy changes you can implement immediately that cost nothing. Every business is at risk of being attacked by cybercriminals. It is essential to know the most cost-effective critical steps you can take right now to secure your organization.

2 "My personal computer won't get hacked, and I prefer using it."

Even if they have antivirus and anti-malware protection, **personal devices are not as safe as corporate ones.** An organization-owned device can be secured by enterprise-class endpoint protection, while personal devices will often run a lower-grade free antivirus service, at best. A device provided by your association will also have security policies enforced, such as password changing policies. Besides not being as secure, personal devices are much more likely to be shared by family members who may not be educated around cybersecurity awareness. They may install personal software or visit a website that might be unsafe, resulting in unknown malware installations.

3 "I'm sure our meeting software is safe."

You might remember "Zoom-bombing" which became a bit of a viral sensation during the COVID-19 pandemic; today meeting security risks are shifting yet again. As organizations increasingly adopt AI-driven meeting software for remote collaboration, they face new cybersecurity challenges. tools can collect and analyze vast amounts of data, including sensitive information shared during virtual meetings. This raises concerns about data privacy, unauthorized access, and potential misuse of information. Additionally, AI features like transcription could potentially be exploited for eavesdropping or extracting confidential data; they could even result in the accidental sharing of confidential information across an organization. Organizations must be vigilant in understanding how these tools handle data, ensuring strong encryption and access controls, and regularly reviewing their security protocols. It's crucial to balance the benefits of AI-enhanced meeting tools with the need to protect sensitive business information.

4 "Our third-party vendors don't pose a significant cybersecurity risk."

Recent trends indicate a rise in third-party breaches. In fact, **49% of organizations reported experiencing data breaches through their third-party vendors last year.** It's crucial to acknowledge that the cybersecurity of your organization is deeply intertwined with that of your vendors. With nearly half of organizations experiencing breaches via third-party vendors, the emphasis on conducting comprehensive security assessments of these partners cannot be overstated. This process should involve rigorous vetting, regular audits, and ensuring that vendors adhere to stringent cybersecurity standards. Ultimately, the security of your data and systems is only as strong as the weakest link in your supply chain. Therefore, developing a collaborative approach with vendors to bolster mutual cybersecurity resilience is essential for comprehensive protection.

5 "Phishing scams are easy to spot and avoid, I'll never fall for that."

Phishing remains a prevalent threat, with **57% of organizations observing frequent phishing attempts.** These attacks have evolved, becoming more sophisticated and harder to recognize, particularly with the integration of AI technologies. Cybercriminals are leveraging AI to create more convincing phishing emails and messages that can easily fool even the cautious user. These AI-enhanced scams can mimic legitimate communications with a high degree of accuracy, making them difficult to distinguish from genuine interactions. The rise in AI-driven phishing tactics underscores the importance of regular, updated training for staff to recognize and respond to these evolving threats. Remember, a single click on a malicious link can compromise your entire network.

6 "Remote work has been around for a while now; it probably doesn't increase cybersecurity risks anymore."

The transition to remote work, while not new, continues to pose significant cybersecurity challenges. With studies indicating that **remote work-related breaches can increase the cost of a breach by over $1 million,** it's clear that remote work environments are not inherently secure. Organizations need to proactively establish robust remote work policies, focusing on secure communication tools and comprehensive cybersecurity training for their workforce. This approach is not just a temporary adjustment but a necessary investment in the long-term security and resilience of the organization.

7 "Our IT department handles all our cybersecurity needs."

While your IT department or provider certainly holds much responsibility for recommending a strategy and the right technologies, they are not the only stakeholders. It is the leadership team's responsibility to:

- Identify critical assets
- Assign scopes of responsibility
- Set and enforce internal policies
- Make security training available to all staff
- Have ready-to-run response plans
- Maintain oversight of the other teams such as IT, service providers and staff.

You know your business better than anyone else, and like most business initiatives, cybersecurity needs to start from the top.

8 "I've already got anti-virus and a firewall. That's enough, right?"

Having the right security tools in place is essential, but that alone is not enough. Cybercriminals will try to find the easiest way into your network, and most often, people are the weakest link. **Regular cybersecurity awareness training is critical** to a successful security strategy and the protection of your financial and digital assets. It will help heighten threat awareness, turn the right behaviors into habit and transform "shouldn't have clicked" into "didn't click." In addition to training, developing and enforcing concrete password policies is also vital. No one should be using the same password for multiple logins, and they should have to change their passwords frequently. You should also require password changes for shared logins when someone leaves your organization. Multifactor authentication (MFA) should be enabled on all systems that allow it. **Strong password policies paired with MFA** help prevent bad actors from gaining access to anything else if a password is compromised.

9 "We use the cloud, and it's automatically secure."

There are many reasons why the cloud is a secure option, such as offering data centers with limited access, added security protocols and encrypted drives. Unfortunately, many security features aren't enabled by default and can result in incremental charges and thus **require an experienced cloud engineer to appropriately secure your systems, keep them available, and do so without breaking the bank.** Additionally, users with weak passwords could potentially make for an easy entry point even in a well-managed system. It is vital to have a security expert review your cloud implementation to ensure all bases are covered and your cloud implementation is safe and secure.

10 "We're too small to need formal cybersecurity policies or an incident response plan."

Surprisingly, over 77% of organizations lack a formal incident response plan. For associations and nonprofits, creating a formal incident response plan and cybersecurity policy is crucial and can be cost-effective. It's more about dedicating time and gaining organizational commitment than incurring large expenses. Collaborating with a reliable IT partner can significantly streamline this process. They can offer expertise and resources to identify vulnerabilities, develop response strategies, and train staff, ensuring a robust cybersecurity framework. This partnership allows even resource-limited entities to effectively secure their operations and data, fostering a culture of cybersecurity with minimal financial strain. No matter the size, every organization should have a documented cybersecurity policy and an incident response plan. These plans are crucial in not only preventing breaches but also in mitigating damage if an incident occurs.

CHAPTER 5

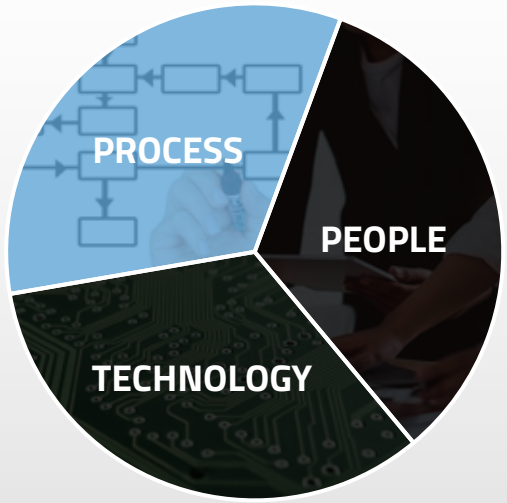
Taking Action With Process, Technology and People

Process: Where is the Best Place to Start?

The right security strategy is different for every organization and depends on your risk tolerance, budget, the types and quantity of data you manage and current security weaknesses. When considering changes to your security practice, you need a balance of process, technology and people. Process (including policies and procedures) are a great place to start because they often don't require a significant monetary investment and most can be implemented relatively quickly.

Policies and Procedures

Creating policies and procedures requires effort upfront to document and distribute to staff. Designate someone in your organization who is responsible for overseeing and enforcing your cybersecurity policies and procedures. There are many to choose from, but we have outlined the **top nine policies and procedures you should focus on.**



1. Remote Access Policy

Your Remote Access Policy document should provide **a summary of the acceptable methods for connecting to your organization's internal networks**. This policy is critical if you have a lot of remote locations or workers. It should outline your organization's guidelines for connecting to public Wi-Fi networks and unmanaged home networks. If you allow employees to bring their own device (BYOD), the procedures for connecting personal devices should be outlined in this document or as an amendment to this document. Personal devices should be required to meet specific hardware and software standards for remote access, including antivirus, anti-malware, software updates, software firewalls and data/device encryption.

2. Email/Communication Policy

This policy covers email, social media, blogs, or other electronic communication technologies. It provides staff with **a guideline of acceptable ways to use your organization's electronic communication mediums**. With many businesses working remotely or hybrid, email is often the primary means of communication for many employees. With the rise of Phishing and Business Email Compromise, we recommend including guidelines for identity verification in your email/communication policy document: Adopt a policy that ensures staff action, such as making a payment, is legitimate by backing it up with a phone call. With everyone communicating virtually, personal information requests may not be red-flagged as readily as before when everyone worked together in an office.

3. Incident Response (IR) Plan

An Incident Response plan will help your organization manage a security incident as it is happening. It is undoubtedly a document you hope never to have to use, but a critical one to have should you ever need it. The purpose of this plan is to **outline the key business decisions, delegations and communications that need to happen during and immediately after a cyber incident**. An incident response plan focuses on minimizing your financial loss and reputation damage.

Public Wi-Fi Security

The ability to work remotely gives employees and organizations unprecedented flexibility, but, like many benefits of technology, working from anywhere can be a double-edged sword. The public Wi-Fi networks that enable staff to work from coffee shops, parks and airports also present a security risk to company data.

There's a lot of helpful information on this topic, but there are also some myths. Learn more about public Wi-Fi security myths, facts and best practices today on our blog.

READ ARTICLE >

4. Disaster Recovery (DR) Plan

Before building a DR plan, perform a risk analysis and organizational impact analysis. Working with your leadership and IT department/provider to complete these analyses will help guide where to focus efforts and resources in the planning process. Your DR plan should **identify your most critical internal systems and outline the key roles and responsibilities to get your essential functions running again**. Examples of disasters to plan for include the loss of your headquarters due to fire or flood, or a major disruption at a cloud service provider (such as Azure or AWS). The DR plan outlines the steps your IT department and other specialized groups will perform to recover your critical systems within your Recovery Time Objective (RTO). The goal is to minimize any adverse impact on operations, and it usually makes up a part of your Business Continuity Plan (BCP).

5. Business Continuity Plan (BCP)

The BCP outlines **all of the steps your organization needs to take to both get back to being fully functional after an incident and to continue operations while your main systems are down**. The DR plan should be a part of your BCP, as it focuses on getting the most critical operations going until full functionality is restored. Your BCP should also include the steps your employees take while the DR plan is enacted, such as recording transactions manually in spreadsheets while your databases are down, or operating an emergency phone bank to process member requests while your website is offline.

6. Acceptable Use Policy (AUP)

An AUP outlines the **limitations and processes required for any employee using a company-issued asset or accessing company-owned data**. Reviewing and signing this document should be part of your onboarding process, as staff should agree to the terms before being granted access to devices and corporate networks. Having and enforcing an AUP can deter staff from using company-issued assets for playing games, running a side business, or engaging in illegal activity.

7. Access Control Policy (ACP)

The ACP outlines **how employee access to your organization's data and information systems is managed**. This policy should include password policies, user access standards, network access controls and software access controls. Additional considerations may include securing unattended workstations and the process of removing access when an employee leaves the organization.

8. Change Management Policy

A change management policy offers a process for organizational changes to operations, services, software and IT. This document should outline **essential communications and training to increase awareness of pending changes**. IT-based changes should also include the possible impacts to the organization as a result of the change, the testing plan and the rollback plan if all doesn't go well. This document aims to take a structured approach to change, minimizing the impact on member service and operations while implementing the necessary improvements to keep your association or nonprofit current.

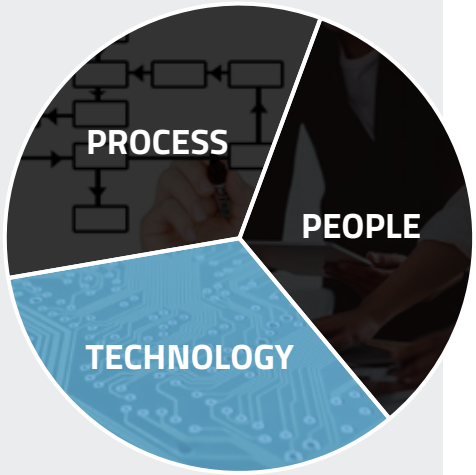
9. Information Security Policy (ISP)

The ISP consists of multiple policies detailing **how your organization intends to protect the organization's IT assets and information**. One essential element is identifying staff accountability as it relates to sensitive data and assets. This document can be signed as part of the onboarding process with the AUP policy.

Many other policies can be adopted as your organization's security practice continues to grow and mature. The nine policies and procedures we have outlined here are an excellent place to get started.

Technology: What Tools Do I Need?

There is no lack of options when it comes to cybersecurity tools. So, where do you start and which ones do you need right now? Our guide below outlines the essential tools that every organization should have, the nice-to-have options, and the top choices every security enthusiast should consider.



Don't Get Caught Without Them! These are Your Essential Tools

When determining your cybersecurity budget, **these tools should be at the top of your list of must-haves:**

Multi-Factor Authentication (MFA)

Authentication is the process of a system confirming the identity of its user. There are three main factors that a system can use to gain this confirmation:

1. **Something you know** (such as a password or PIN).
2. **Something you have** (such as a code generated by an app or texted to your cell phone).
3. **Something you are** (such as your unique fingerprint or retina scan).

When you hear the terms "two factor authentication" or "multi-factor authentication," they refer to a system using checks from two of these factors, or even all three. It is far easier for a criminal to bypass a single-factor form of authentication (such as a password) than it is to bypass multi-factor and so using multi-factor whenever it is possible will significantly improve the security of your systems. (Note that using two items from the same factor, such as a password and a PIN, which are both "something you know" does NOT qualify as multi-factor authentication!).

Robust Firewalls

Your firewalls serve as your **first line of defense against cybercrime attacks**, and a firewall should be logically positioned in your network at every Internet connection. Look for firewalls that include intrusion detection systems (IDS) and intrusion protection systems (IPS), which work to recognize attacks based on web traffic behavioral analysis, threat signatures, and suspicious activity. Features like application awareness and advanced threat protection, commonly found on Layer 7 firewalls, are also important. Application awareness helps the firewall detect hidden threats. It also allows you to block certain software features without blocking the entire software (allowing LinkedIn but not LinkedIn chat). Advanced threat protection means having antivirus and malware protection that is upgraded automatically as new threats are discovered. (Note that you need firewalls at ALL Internet connections! If you have servers in Microsoft Azure or Amazon Web Services, you need a virtual firewall to protect them too!)

Email Filtering

Most email providers have a built-in feature for flagging and filtering spam, but they are not smart enough to catch emails with malicious links or infected attachments. A third-party email filtering application is recommended to **filter out not only spam, but also these more malicious emails**, keeping email clean and safe.

Anti-Ransomware

Ransomware is the most prevalent cybersecurity threat out there. It is incredibly dangerous and destructive, costing incredible sums of money for the organizations that fall victim. An anti-ransomware software can **identify the act of files being encrypted, stop it, reverse it and notify your security and IT teams**.

Protecting Your Organization From Email Compromise

While phishing scams have been around for over a decade, Business Email Compromise (the act of a criminal gaining access to one of your staff members' email accounts and using it to spy on communication, impersonate your staff member, commit financial fraud and reset bank passwords) is now the most profitable type of cybercrime. Business Email Compromise (BEC) can be prevented with proper security controls on your email system, but once it happens, it can be impossible for either spam filters or human beings to identify these imposter emails. Learn more about how to protect your organization from business email compromise today on our blog.

READ ARTICLE >

But Wait, There's More! Here Are Additional Protections You Can Implement

If you have already implemented the must-have tools noted above, and you have the budget to reinforce your security a little more, these tools are an excellent next step:

Password Keeping Software

When you implement password security policies, you may hear grumbling from those who struggle to recall passwords — especially if you use a lot of software and require frequent password updates. Implementing password keeping software at the organization level can help **increase the acceptance of new password policies and prevent lost productivity. It is also a great way to manage shared accounts, increase the likelihood of longer, stronger passwords and prevent staff from writing down their passwords on sticky notes or other easy-to-compromise locations.** A password keeper that your organization supports and manages is ideal, as it allows you to access those passwords even when an employee leaves the company (and helps itemize which passwords you need to change). (Note that even if you don't have a password keeper at the organization level, you should set policies for your staff using personal password managers.) There are advantages (including many listed above) and downsides (the passwords are stored in a system your organization doesn't have direct control over), but either way you should have an established policy on personal password managers for your staff to follow.

Vulnerability Scanning

Your IT department should already be managing and deploying patches regularly to your workstations, servers and networking equipment. Vulnerability Scanning takes it one step further to **actively scan for known weaknesses that could indicate a missing patch, a misconfiguration, or a back door implanted earlier by a cyber criminal**. Vulnerability scanning helps to identify vulnerabilities before cybercriminals can take advantage of them so you can take steps to remedy them.

Phishing Simulation

Once you have delivered security awareness training to your staff, it is a great idea to **test their ability to detect phishing attacks safely**. Identifying those who are more vulnerable to falling victim to phishing can help determine the need for additional training. Regular simulations are also an excellent way to remind your employees to always be on their guard.

Dark Web Monitoring

Dark Web monitoring is a service that **monitors the hidden parts of the Internet (commonly called the Dark Web) for databases and forum posts of stolen usernames, passwords, credit card numbers and other personal information**. These services can notify you if an email address associated with your organization is found in this material, allowing you to take action such as warning your employees, changing passwords and protecting credit and finances.

For the Security Enthusiast: High-End Tools

If you have a mature security practice that you are looking to reinforce even further, these tools are for you:

Penetration Testing

Penetration testing aims to **exploit the weaknesses in your systems** (such as those found in a vulnerability scan) similarly to how a cybercriminal would, but by a trained cybersecurity professional working for you. These "ethical hackers" will test your vulnerability management and other security controls to see how far they can penetrate your network and will then provide a penetration report so you know what vulnerabilities they exploited, how far they got and what you can do to close these security holes.

Device Encryption/Encryption at Rest

Encrypting your data **prevents visibility in the event of unauthorized access or theft**. It is important to encrypt data in motion, such as when sending an email or sharing a file. Encrypting data at rest is also becoming more common, preventing visibility when the hardware or virtual disks are stolen or disposed of.

Security Information and Event Management (SIEM)

SIEM systems are designed to **integrate information and logs from various sources (including firewalls, switches, servers, workstations, your email system, etc.), correlate that data and then provide actionable and timely alerting** to your IT team of possible cybersecurity events. A SIEM not only helps IT respond faster to an event but by analyzing the event, it also helps your IT team prevent similar attacks from happening again in the future.

Cybersecurity Frameworks

This Ebook address the most common risks and the most impactful changes you can implement at your organization, but no Ebook can replace a true Cybersecurity Risk Assessment based on a Cybersecurity Framework.

A Cybersecurity Framework is a comprehensive look at all functions of cybersecurity (inclusive of people, process and technology) that should be considered throughout your organization, such as the one provided by the National Institute of Standards and Technology (the NIST Cybersecurity Framework).

For more information on how to apply a framework to your organization and conduct a Cybersecurity Risk Assessment, contact designDATA.

CONTACT US designDATA >

People: What Role Does My Staff Have?

The Human Firewall

Besides having well-documented policies and procedures paired with essential tools, **training your staff is one of the most critical cybersecurity strategy elements**. The "human firewall" is the last line of defense when the technology and tools have failed to stop a threat from getting through. Educating your employees regularly to keep security awareness top-of-mind is the vital last piece of the puzzle.

According to a report by KnowBe4, when no security awareness training had been conducted,

> **1 out of 3 employees was likely to click on a suspicious link or email or obey a fraudulent request.**

READ MORE >

The report also notes that "no organization performed well without training. Very few industries were under 30% in 'Phish-Prone' employees." When the same organizations were tested again within 90 days of administering security awareness training, the percentage of Phish-Prone employees went down to 14.1%. After a year of ongoing training, the rate of Phish-Prone employees was down to 4.7%.

These dramatic decreases highlight the importance of regular security awareness training to keep employees educated and security conscious.

Getting Started

Where Should You Go From Here?

No one wants to receive a phone call in the middle of the night because they've had a security breach. Understanding your current weaknesses and risk tolerance is a significant first step towards building a cybersecurity strategy that provides you peace of mind.

We sincerely hope this Ebook provides the information you need to overcome the misconceptions and understand where to begin your cybersecurity journey. Don't get caught unprepared; **reach out to one of our cybersecurity experts** to book an assessment and start protecting your business today.

> **Get started by contacting designDATA today 301-921-6696 or visit our website at designdata.com/cybersecurity-solutions/ to learn more.**

designDATA

610 Professional Drive
Suite 102
Gaithersburg, MD 20879

1425 K Street NW
Suite 500
Washington, DC 20005

(301) 921-6696

www.designDATA.com