AXXYS TECHNOLOGIES

The Importance of Business Security

www.axxys.com

Table of Contents

Finding Gaps in a Security Risk Assessment

Cyberattacks cause an unprecedented level of disruption for business owners. While it may seem as if hackers use highly complex tools to disrupt business operations, steal highly sensitive data, and even steal money or financial information – more often than not they are using very simple tools and strategies to make a big impact.

According to Symantec, malicious emails were the preferred weapon of choice for cyberattacks in 2016 with one out of every 131 emails sent being malicious in nature. New ransomware attacks have seen a 36% increase in infections over the past year alone.

What makes this possible are gaps in your own network security, which include your operating systems, email, and even your wireless network. Now, more than ever, is the time to take a hard look at your network security infrastructure and processes to ensure maximum protection against cyber threats.

> "In 2016 with one out of every 131 emails sent was malicious in nature. New ransomware attacks have seen a **36% increase** in infections over the past year alone."
>
> — Symantec

Understand What's at Stake

Over the past eight years more than 7.1 billion identities have been exposed in data breaches. Research from Kaspersky shows that 26% of DDoS (Distributed Denial of Service) attacks create such massive data loss that companies affected by it will never recover. Given that fact and the reemergence of malicious emails becoming fairly effective again, the importance of network security cannot be overstated when such basic cyberattacks are so effective.

If your organization's network security strategy and measures are inadequate, you are putting your customers, your employees, and your company at great risk. If your company were to fall victim to a major cyberattack that resulted in massive data loss and downtime, there would be potential negative consequences for your organization.

Here are just three such negative consequences you could expect:

- **Federal compliance violation penalties/fines for loss of employee and client data**
- **Loss of trust and reputation among employees and customers**
- **Loss of the business due to inability to recover**

How do you know if your organization is poised to withstand the network security threats of today? What about the network security threats of tomorrow?

The only way to truly know whether your business is vulnerable or not, and how vulnerable it really is, would be to conduct a thorough network security assessment – or audit as it's called. Network security audits allow IT professionals and businesses to identify where network security shortcomings are, the best way to plug those holes, and identifies all devices and equipment within your IT infrastructure. The audit will also determine whether the equipment and software your organization currently has in place is capable of supporting the necessary security solutions.

The Benefits of a Network Security Audit

Every day there seems to be a news report about the latest network security threats accompanied by verified stories of actual data breaches, loss, and downtime as a result of those threats. As easy as it is to simply say, "Yes, I will take cybersecurity seriously today!", sometimes the most difficult part is knowing where to even start.

Security gaps and the dangers they bring are a real thing, as has been highlighted throughout this resource. It's no longer enough to understand the risks associated with those gaps and incorporating a 'path of least resistance' type of strategy for network security. Off-the-shelf solutions are wholly inadequate for business purposes and they won't come close to helping you understand exactly where your security risks are.

That's why it's important to work with IT professionals, true experts in the field, to conduct a thorough network security audit of your IT infrastructure and processes. The benefits of doing so aren't just to help you identify and close any security gaps within your IT network before they are discovered by hackers. Identifying those security gaps is certainly a major part of it but supplemental benefits include being able to know exactly what employees need to be educated on regarding present-day risks, while also recognizing and understanding your organization's digital footprint.

Automatically Backup Data and Systems

This should be a no-brainer but more often than not, automatic data backup processes in place are inadequate. Part of it has to do with keeping data backups on-site in an unsecured manner and a lack of backup testing. Another part has to do with only maintaining one backup, when you should have several – basically, backups for your backups. And, finally automatic backups aren't happening as often as they should be. There are ways in which backups can happen automatically every time something on your network changes, and part of that has to do with utilizing the cloud responsibly.

Other than working with a dedicated team of IT professionals, backups are your ace in the hole when dealing with critical data loss, breaches, or downtime. |

Contact Us

Utilizing Network Security Auditing

If you don't know where your weaknesses are, how do you know what needs to be done to fix them? The fact is, you don't and that's why one of the first things you should do to protect your business is to bring in outside cybersecurity consultants to perform a comprehensive cybersecurity review of your network. Utilizing network security auditing from a dedicated group of IT professionals will provide you with the necessary information to make sound technology decisions for the future.

Those decisions made easier by network security audits include where to direct your efforts in closing any network security gaps your organization may have, whether your data backup/recovery policies and procedures need sprucing up, and even if you're doing enough to educate and train employees on the potential cyberattacks.

At a minimum, a cybersecurity review should cover the following areas:

Your IT Infrastructure

This involves reviewing in great detail how your organization is structured and includes the IT infrastructure you currently have in place. Is the equipment and software you currently have of high quality and possess the capabilities to serve your cybersecurity needs, or are their gaps and pitfalls that need to be addressed? Sometimes it's as straightforward as complementing your existing IT infrastructure with a few additional pieces of equipment or software, and then getting them all working in concert as a cohesive unit.

External Scans for Vulnerabilities

Where are the weak points in your existing cybersecurity systems? That's the purpose of doing an external scan. Does your network have ports open and accepting any and all web traffic types when it really should be closed? Is your network security software configured and updated to detect some of the latest malware and ransomware programs being passed around the internet right now? That's what you need to find out so action can be taken where appropriate.

Full Inventory of Devices and Software

Computers, routers, phone systems, printers, smartphones, tablets, and even the fax machines all maintain connections to your network. Given that your business IT network is one of the most valuable assets you own, it's important to maintain a full inventory of all devices and software your company has. Maintaining this inventory system can also contribute to significantly reducing the effects of network downtime because you are more readily able to identify problem devices and software for faster resolution.

> "**64% of Americans** cave in to digital extortion demands."
>
> — Symantec

Best Practices Documentation

The size of your network will determine just how expansive your best practices documentation needs to be. Additionally, best practices documents should include everything that's relevant to your network and overall IT infrastructure. It's also why no two best practices documents will ever be the same.

If your network is small with a single firewall and just a couple switches, there isn't a whole lot to document. On the other hand, a larger network that consists of multiple access points, half a dozen servers and network switches with multiple people monitoring them – a much more expansive document is necessary to highlight the critical aspects of your network.

Data Backup and Recovery Policies

The best tool at your disposal in times of critical disaster or failure is your data backup and recovery policy. There is a multitude of ways to backup and recover data, but which one is right for your business? That's what needs to be addressed and determined during any audit. A weak data backup and recovery policy simply means it will become that much more difficult to recover valuable data than it really should be.

By the Numbers – Cybersecurity Research Worth Mentioning

What's really going on inside the networks of organizations today can sometimes be difficult to truly assess. That's why it's important to take a look at legitimate industry research and surveys conducted by reputable cybersecurity research firms for insight.

Ransomware and malicious emails are the two most popular ways in which hackers infiltrate company networks. More specifically, Symantec reports 64% of Americans cave in to digital extortion demands. The average across the globe is just 34% and considering the average ransom demand from ransomware infections is roughly $1,100 per victim – ransomware has become even more profitable for those that run the scams year-over-year.

Another area in which companies have become incredibly vulnerable is with cloud infrastructure and applications. The fact is, many organizations simply lose track of how many different cloud applications are in use within their IT infrastructure. Symantec's Annual Threat Report highlights that many CIOs believe their companies only use around 40 or so cloud apps for business productivity purposes. The reality is much more frightening as companies, on average, are actually utilizing closer to 100. The reason that's scary for companies everywhere is because without conducting regular network security audits, you'll never know what you are, and are not, running and whether the cloud applications used open you up to risk.

Results from the Black Hat Security Survey reveal that only 64% of companies actually run cybersecurity drills annually, even though 92% of respondents believe running such drills would help companies prepare for potential cyberattacks and threats. |

Contact Us

shift

A Cybersecurity Audit Lets You Find Weaknesses First

Network security is serious business and maintaining tight security controls over your network, which includes all of the data and information your company is responsible for, means treating it that way. Security breaches can occur because people aren't paying attention to the websites they visit, continue to use weak password structure, or opening attachments in emails they really shouldn't be.

If breaches do occur, regardless of how, the latest studies have concluded it can take as long as five months before those breaches are actually discovered. There have been some cases, such as the Trump Hotels and Target hacks, where it took nearly double (and even triple) that amount of time before security breaches were detected. That's why it's important to have security measures and IT professionals in place to help defend against such intrusions and events 24/7/365.

If that's not enough to get your attention, think about this. The Ponemon Institute released a recent study where the global average cost of a single data breach has an average price tag of nearly $4 million and the average cost for each lost record due to data breaches has risen to approximately $160.

Identifying where your network security weaknesses are before hackers do is paramount to successfully defending against the wide variety of cyberattacks online today.

An effective cybersecurity audit will, at the very least, provide indepth information on your overall IT infrastructure, whether your hardware and software have any vulnerabilities, provide a full report on all devices and software connected to the network, update best practices, and review backup and data recovery processes.

Proactively Monitor Your IT Network

A part of conducting a cybersecurity audit includes acting on the weaknesses found. That, of course, means being proactive about network monitoring and support. There are numerous benefits to proactively monitoring your IT network. Other than having the ability to ensure the health and integrity of your network in general, you are also able to minimize your risk. Doing so effectively does require having someone available 24/7 to keep an eye on things for your organization, which usually means working with a dedicated IT partner. By doing so you can guarantee the security and safety of your company and the data it collects.

Proactive network monitoring helps minimize risk by:

- **Monitoring all update activity and ensuring all updates are properly installed**
- **Monitoring firewall activity, hacking attempts, and whether spikes in traffic are relevant or spamming attempts**
- **Monitoring all application services such as Exchange, HTTP, file sharing, etc. to ensure they are running properly**
- **Monitoring all backup and recovery testing statuses**

> “The global average cost of a single data breach has an average price tag of nearly **$4 million**.”
>
> — Ponemon Institute

Prevent Unauthorized Access to Your Network

There’s no such thing as a perfect off-the-shelf network security solution or software. Given that the latest ransomware threats alone can cost victims an average of $1,077 per instance, it’s more important than ever to prevent unauthorized access to your network. Doing so is, once again, just another part of identifying your network security weaknesses and fixing them before hackers can exploit them.

According to Symantec’s latest report, the number of ransomware detections increased by over 100,000 from 2015 to 2016 and only figures to increase again in 2017. And it’s not just ransomware - as mentioned previously, malicious emails and phishing scams have made a comeback in a huge way over the last year with over 4,000 email attacks everyday since January 2016.

So, how can you take extra measures in preventing unauthorized access to your network?

In addition to setting up strong passwords and getting serious about keeping your operating system, software, and hardware updated at all times – you should also be enforcing data security policies with a vengeance.

Keep Your OS, Network Connected Devices, and Software Up to Date

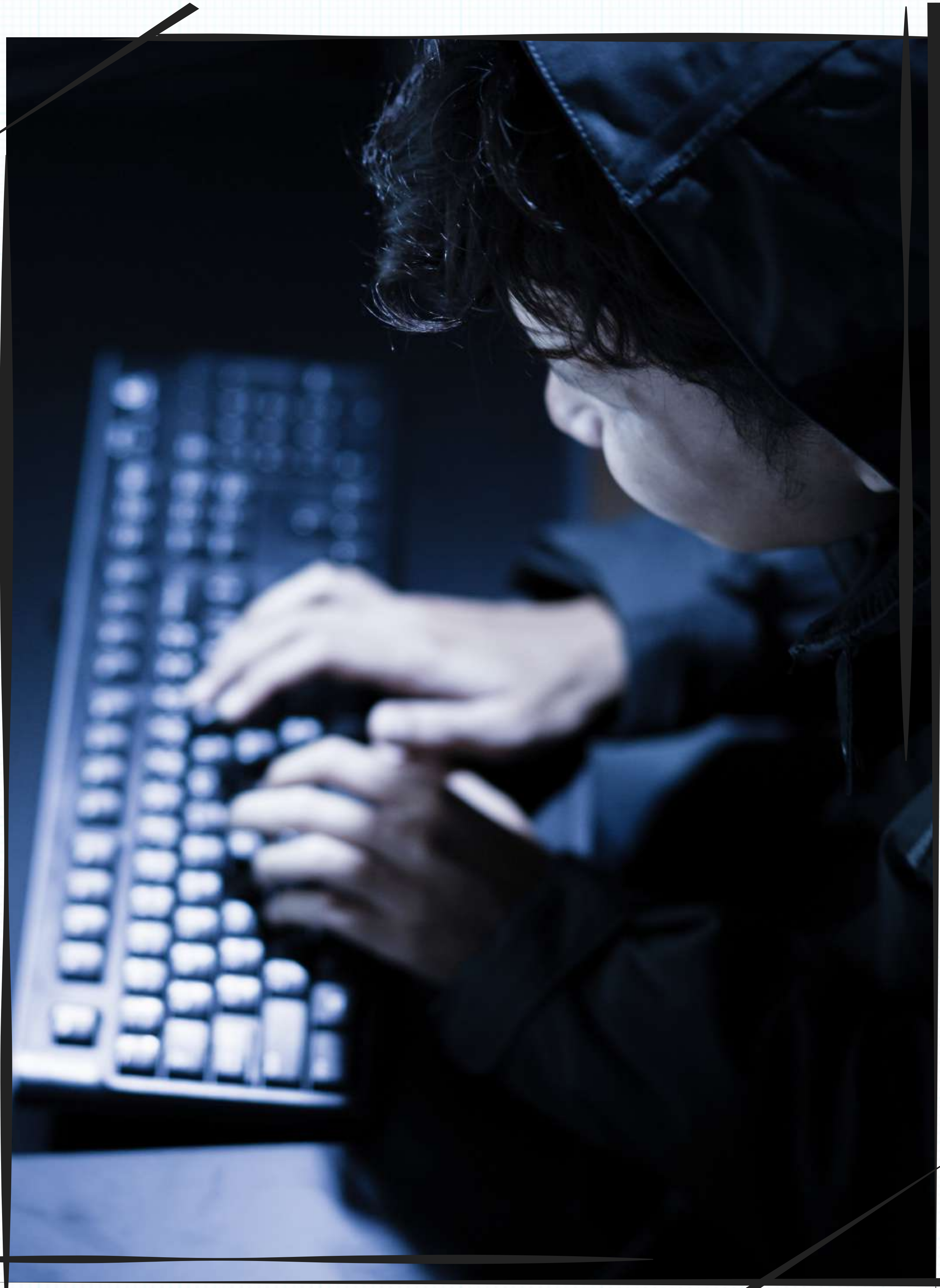
It's not all that difficult to take the hardware and software we use on a daily basis for granted. Especially when the computers, software, and other business productivity tools used by employees aren't actually owned or maintained by those who actively use them. A thorough cybersecurity audit will uncover which network connected devices need updates, what software being used is currently two versions behind the most recently patched version, and whether or not your operating system is configured properly for network security purposes.

When businesses don't take the time to have IT professionals properly and proactively maintain the technology being used every day, it's like an open invitation to anyone with even rudimentary hacking skills or knowledge. Sometimes the easiest thing that can be done to prevent hacks, data breaches, or even unplanned downtime is to take care of the simple tasks like patching and updating drivers, firmware and software.

Keeping your IT network updated with the latest software updates, patches and drivers for hardware is critical to network security. If your organization doesn't have the expertise to handle these matters internally, don't be shy about contacting an IT professional like Axxys Technologies to help keep your business protected.

Discovering where your weak points are as it pertains to your network security is the only way to know if you're prepared for anything that may come your way. Knowledge is power, after all, and plugging up the holes in your business security is the only sure-fire way to keep the undesirables out. |

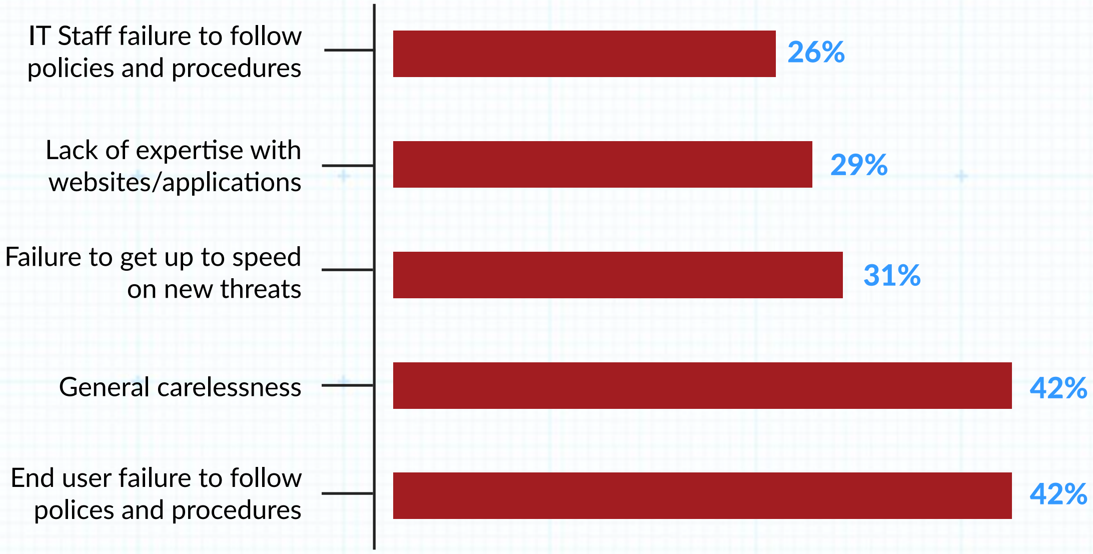
Contact Us



The Biggest Threat to Network Security Comes from Within

It's easy to think of network security threats facing companies and imagine hackers and outside sources being the leading cause of data breaches, critical downtime, and even hardware failure. However, the IT Policy Compliance Group says 75% of ALL data loss is due to human error. In fact, human error can be attributed to the various activities that lead to the majority of data breaches, data loss, and general security incidents.

Top Examples of Human Error



How to prevent human error from causing data breaches and loss:

- **Improve data security education efforts**
- **Implement access rights and privilege strategies**
- **Run simulated phishing programs for training purposes**

Every year companies go through the process of implementing the latest security technologies and strategies in an effort to prevent data breaches, improve general network security, and incorporate better best-practices into daily business operations. And yet, regardless of the latest and greatest in network security or antivirus software and strategies, it's still difficult to fully protect against human error and inattention to detail when it comes to network security.

That's why creating an effective cybersecurity training program for current and prospective employees is vital to enhancing network security efforts. Employees who are trained and provided the necessary resources to identify potential phishing scams, malicious emails, and other hacking efforts are less likely to make mistakes that cost valuable time, money, or cause downtime and data loss.

The Dangers of Unknown Security Risks

With so many network security risks out there, if internal teams aren't aware they exist and don't know what to look for – how could you possibly expect them to help the company combat them? Employees can, and oftentimes do, unknowingly pose the biggest security risks to the company they work for simply because they don't know any better.

Unknown security risks your employees should be educated on take on many forms, but here are some of the most common:

- **Social engineering attacks designed to gain confidential information from an unsuspecting employee**
- **Virus software that hasn't been updated in months because the seriousness of the situation doesn't prompt immediate action on the person overseeing it**
- **Downloading files from the internet from untrusted, or approved, sources**
- **Failure to properly secure and catalog company devices such as laptops, smartphones, and tablets**

With the right training, all of the aforementioned network security threats become a bit less concerning because employees will know what to look out for and how to address potential threats.

Three Easy Training Types Any Organization Can Implement

When it comes to actually educating employees on the do's and don'ts of network security, where do you even begin? Each person that is a part of your organization will have varying degrees of network security knowledge and training. In fact, some will actually have no prior experience or training at all – and these are the employees you'll really need to spend some time focusing on.

> "Every year companies go through the process of implementing the **latest security technologies and strategies** to incorporate better best-practices into daily business operations."

Security awareness training can be implemented in a number of ways, either in a one-on-one setting or in a classroom environment. Obviously whether your company is able to offer training depends on the resources available to deliver any kind of specialized training programs. Regardless of resources available, however, there are three specific kinds of network security education programs just about any company can integrate into daily business operations:

- **Providing access to existing online training programs and materials from trusted and certified sources.**
- **Setting up a "Helpful Hints" system that provides pop-ups and feedback when someone tries accessing certain sections of company data, or when they login to their computers throughout the day.**
- **Visual aids and flyers that are prevalent around the organization and routinely handed out to individuals and teams during meetings, or during normal working hours.**

Getting the Right Training Programs in Place

It would be foolhardy to believe a company only has one specific area they are weak in when it comes to network security. It’s not because people are intentionally being obtuse, but rather because the vast majority of systems are interconnected. That means if one device or one piece of software is vulnerable then the entire IT ecosystem is vulnerable. What makes security awareness training programs successful has less to do with how deep the pockets of the company are, and much more to do with how effectively the necessary information is delivered.

> “**75% of ALL data loss** is due to human error.”
>
> — IT Policy Compliance Group

First and foremost, network security training must absolutely be incorporated into any new employee orientation. By doing so your organization not only makes it readily apparent just how serious network security is, but the seed has been planted for all new employees that it is something they are expected to be mindful of.

Taking things a step further, training should be developed for specialty roles where specific types of employees are responsible for more of the niche operations within an organization. For example, if an IT professional is hired to monitor any and all incoming and outgoing internet connections within the organizations, it doesn’t do much good to have them spend time troubleshooting the general computer issues employees tend to have from time-to-time – tickets submitted for lost passwords come to mind.

Reinforcing Network Security Training and Reeducation

Once you have a plan in place for implementing the right network security training programs for your employees and organizations, how do you keep everyone's knowledge base and skills up-to-date?

There are any number of ways to do just that, but you must also understand the company culture and what is and is not deemed acceptable. One way to reinforce network security training education is through positive feedback. Seems simple enough, yet it may not be for some employees to remember and maintain that critical knowledge. From there you could graduate up to rewards such as gift cards or company gear of some kind if employees score a certain number on follow up tests or modules.

In reality though, repetition is likely the best course of action for reinforcement of network security education. Create and distribute announcements throughout the company via email and regular newsletters or flyers if the company does those. Only through being exposed to the culture of the company in a way that clearly states and outlines what the expectations are regarding network security will employees keep it top of mind.

Enforce Data Security Policies

With human error attributing to the majority of data breaches (because we're human and we make mistakes), it's inattention to detail by employees that allows hackers into company networks. However, if employees aren't educated and trained on what to look for then how could they possibly know any better?

That's where actually enforcing data security policies and educating your workforce on those policies, including network security best practices, come into play. Some of those policies should include enforcing password resets on company-owned devices every 30 days. They could also include the ability to remotely lock or wipe those devices in case an employee loses them or they are stolen.

After all, what's the point of having data security policies and best practices documented if you're not going to enforce them?

You can no longer be satisfied doing the minimum when it comes to network security and feel confident that your organization is protected. Effective business security takes a bit more effort these days.

Why You Can't Afford to Overlook Security

Most people will agree that proactive solutions are more ideal than reactive solutions. Preventing a disaster is much easier and more affordable than an intensive clean-up and reconstruction. Your network security is no different. It isn't enough to respond to an attack; with 60% of attacked companies closing their doors, your business could be collateral damage.

Cyberattacks are on the rise. They are common and expensive. So, how do you protect yourself? According to CSO, cybersecurity spending will increase by $1 trillion in the next five years. The investment to secure your network is minimal compared to the devastation you could see from a compromised network. Working with Axxys to create and enact a plan will guarantee your data and company are safe from threats. |

Contact Us

AXXYS
TECHNOLOGIES

Since 1987, our dedication to innovative solutions and uncompromised client support has always remained constant. We change the way technology propels your business – together. By taking a collaborative approach to the way we engage our clients, we get to know each other better – because the better we know each other, the better we can help each other succeed.

AXXYS TECHNOLOGIES

Corporate Headquarters

5850 Granite Parkway, Suite 700
Plano, TX 75024

214.297.2100
info@axxys.com

www.axxys.com