Effective Data Security Takes More Than Just Technology

Synoptek®

“Cyber attacks target vulnerabilities in human psychology more so than the victim’s technological sophistication.”

OVERVIEW

From the earliest days of networked computing, many have chosen to believe that securing their network and their data is as simple as putting up a firewall. The reality is that the firewall is perhaps the midpoint of a chain of steps which must be taken to assure optimal protection. Each step in that chain has the potential to be your weakest link, and, as always, that determines how strong the entire chain is.

In this white paper, we’re going to work hard to demonstrate to you why it is all but impossible for a company that doesn’t “do” network security for a living to adequately protect their own network. You can throw many of the technology tools we’ll talk about at the problem, but fully securing a network and the data that moves across it takes more than just tech. It also takes people with the insight to recognize dangerous patterns and the resources to analyze those patterns and keep you ahead of threats.

If you feel that you’re sufficiently familiar with the fundamentals of data and network security, please feel free to skip down to “**Why Companies Choose Managed Information & Data Security”**

GETTING STARTED - SECURITY POLICIY

Putting up a firewall without having a security policy is almost pointless, since the role of the firewall is to enforce your security policy.

You need to start by determining the business rules that will govern the use of data and network systems in your organization. Which users can access what data assets? Which external connections will be allowed into the network, and which applications may be run that access network resources? Which network protocols will be used to connect with other hosts? What internet protocol (IP) addresses will be allowed access?

So far, the rules we’ve listed are all configured into your firewall and other security systems for enforcement. There are also rules, however, that will not be as easy to enforce. These are the rules that must be followed by people.

How will passwords be structured? How often must they be changed? What types of files may or may not be introduced into the network? How will people sharing their passwords with others be dealt with?

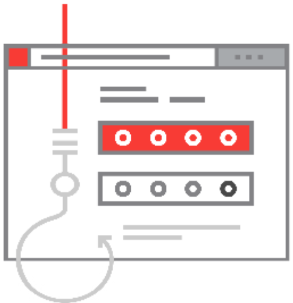
Your Data & Network Security Policy informs and configures every step of the data security chain.

The Data Security Chain

Some like to begin at the beginning, and others prefer to begin with the end in mind. In this case, both are pretty much the same. At the beginning of the data security chain is a user. At the end of the data security chain is a user. It may not be the same user at the same endpoint, but the path is very much the same.

4 IN 5

Think it is likely or very likely that their enterprise will experience a cyber attack this year



53% OF ENTERPRISES

EXPERIENCED MORE ATTACKS this year than in the year prior

AUTHENTICATION – How do we know that the user attempting to access our network is who they say they are? The answer is, we challenge them to give us their Identification code (ID) and their password. This actually constitutes weak authentication, mainly because the top 10 passwords in use in 2016 are the digits 123456789 in various portions and both directions, the number 111111, and the words “qwerty” (top left row of a keyboard) and “password”. Yes, users can be lazy.

Stronger authentication requires the use of multiple challenge factors, including token devices that generate a random number that lasts for 60 seconds when activated. That number is generally added to the password to create a complete multi-factor authentication (MFA) code that combines something the user knows with something they physically possess. The password used no longer really matters. Other MFA devices use facial recognition, fingerprint, or other biometrics.

Identity Theft is highly prevalent in the consumer world as well as the corporate world. This can partly be attributed to the popular use of very weak passwords. In the corporate world it can also be attributed to the carelessness of many users who write their passwords on a “Post-It” note stuck to the bottom of their keyboard or even on the front of their display monitor. Users must constantly be encouraged to provide better protection for passwords. MFA eliminates this concern effectively. Given that 60% of all attackers are actually insiders who have stolen passwords, this one measure could prevent almost two thirds of exploits that may occur on your network.

AUTHORIZATION – Once properly identified and authenticated, the user can now be assigned access to network resources not only based on their individual identity, but also on their role in the organization, and on their current location. Some companies prefer to restrict certain data assets when users are not physically on company premises.

NETWORK ACCESS CONTROL (NAC) – Now that we’ve confirmed who the user is, we also need to approve the device they are using to access the network. Some devices have insufficient internal security to be allowed on the network. Some may already have viruses or other malware running on them. The network wants to know that the device has been approved for access and will interrogate the device to determine whether or not it can be permitted to connect.

INTRUSION DETECTION & INTRUSION PREVENTION SYSTEMS – Data moving across a network moves in packets. Intrusion Detection Systems (IDS) inspect the contents of these packets to determine if they contain anything malicious. When something potentially dangerous is found, the IDS alerts system administrators to take further action. Intrusion Prevention Systems (IPS) go further and can themselves block malicious flows and take other actions to stop the malicious content from entering the network.

The scanning technologies used for IDS and IPS can also be used very proactively to scan for potential attackers who are seeking the best way to penetrate your network. An attacker will usually spend weeks or even months searching for your vulnerabilities before they actually attack. In the hands of an experienced expert, network scans can spot these searches and shut them down before they have a chance to attack.

FIREWALL – The most important component of your security strategy lies in your security policy, the set of rules that govern what connections may or may not be allowed to enter your network based on identity, IP address, protocols, applications, or other criteria. Your firewall may be configured to enforce all those rules.

Many large networks have been brought to their knees recently using Distributed Denial of Service (DDoS) attacks in which the attacker enlists thousands upon thousands of devices to bombard your firewall with requests. The sheer volume of requests overwhelms your systems which simply shut down due to the overload. Keep a network down long enough and the cost of downtime starts to increase geometrically.

ANTI-VIRUS/ANTI-MALWARE – Thousands of new viruses and other malware are being “released into the wild” every day. Experts work diligently to identify new ones and provide “signatures” that anti-virus software can use to identify and block these exploits from entering your network. The work of those experts is hugely valuable, making the responsibility to keep anti-virus signatures on your network fully up to date that much more important.

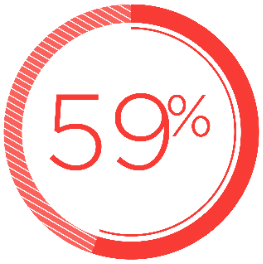
One of the most frequent attacks in recent times have been “phishing” attacks in which an email is sent to one of your users. Because there is no malicious content in the email it easily makes its way through your defenses. Then it attacks the most vulnerable part of your network, your user. The request in the email seems genuine and valuable enough, and it’s easy enough to click the link the user is asked to click. Studies show that 23% of users routinely open phishing messages, and 11% will click on links or attachments that wreak havoc. Once they do, the attacker can easily drill through your network defenses and exploit your data assets with all manner of viruses, worms, and other malware.

ENCRYPTION – Now the access request has made its way through all your defenses and is about to access data from your servers. The final and most important layer of protection is the encryption of your data. If the user accessing the network has your encryption key, they will be able to decrypt the data at their end. If they do not, they will receive gibberish, completely garbled data that they cannot use.

From here, the user’s original request may simply retrace its steps back to the user to retrieve requested data and return it to their client device. In other cases, such as messaging, the data may make a similar journey to another user.

Each of these steps requires extensive maintenance, constant attention, and maximum vigilance. Anti-malware signatures must be kept current. New security patches coming from operating system and application vendors must be evaluated and applied promptly. Encryption keys must be supervised and managed.

CYBER SECURITY THREATS



Of enterprises are concerned with **INTERNET OF THINGS IN THE WORKPLACE**

53% **OF ENTERPRISES**

Have a formal process to deal with **RANSOMWARE ATTACKS**

The Need for Expertise

Those organizations setting out to handle data and network security themselves need to carefully consider the expense involved. Far beyond the hardware and software required to run MFA, NAC, IDS, IPS, firewall, anti-malware, encryption and more is the expense of having the highly-trained experts on staff required to optimize the effort.

Beyond keeping everything running, highly-experienced (read as "highly-expensive") experts must keep a constant eye on the tremendous amount of global security data being collected every day. Giving them access to a global security database is an expensive item unto itself, but their ability to compare their own network scans with the exploits and other signatures available to them in the global databases is critical to their ability to identify and defend against the most dangerous exploits of all, "zero-day" exploits. Brand new, nobody has necessarily had time to identify these yet and the only way to protect against them is to have a true expert hunting them down constantly.

BIGGEST SKILLS GAP IN TODAY'S SECURITY PROFESSIONALS

25%
Cloud Security

52%
Intrusion Detection

17%
Network Monitoring

Why Companies Choose Managed Information Security

As covered in previous sections of this paper, comprehensive IT security requires a laundry list of resources and applications, including: DDoS protection, intrusion prevention systems, web application firewalls, data loss prevention, SIEM, threat hunting, end-user training, and security policy creation.

This list can be overwhelming for many companies that don't have a large cyber security budget nor the internal expertise to properly configure and manage these programs. In this scenario, it makes sense why so many firms are choosing to partner with a Managed Services Provider (MSP) that can provide an advanced managed IT security solution to address all of these items for a flat monthly fee.

A few examples of when it makes sense to use a Managed Security service from an MSP:

• Your IT security team is understaffed and cannot monitor your network and systems 24x7

• Building an IT security team and internal SOC doesn't make financial sense for your needs

• You have regulatory compliance requirements and you do not have the resources to meet them

• You need help managing and monitoring your 3rd party vendors

Managed Security services can help you in the following scenarios:

• Monitoring Only – alert and inform your organization about security incidents

• Monitor & Manage – monitoring of log data and providing the necessary remediation to secure your environment if required

• Managing Technology – configuring firewalls, using AI to investigate anomalous behavior, or making changes to a security device

The advantages of using an MSP to manage your IT security include:

• Access to IT security expertise and threat intelligence

• Established SOCs to validate and send alerts on active security incidents

• Less expensive than building a security team in-house

As the evolution of technology and our digital ecosystem grows more intricate, cyber criminals have more possible attack vectors—and businesses of all sizes have more areas to defend, including a growing number of connected devices, cloud computing solutions, and shadow IT applications.

Synoptek Managed IT Security as a Service

Just as the steps just reviewed can be seen as "layers" of the network to be secured, the best, most-effective security solutions also provide layer upon layer of protection. Synoptek's approach starts at the same beginning and end we've already examined and proceeds accordingly.

The result is a comprehensive program that puts full and equal attention behind every step of the chain of security:

- **Endpoint –** Often considered the point of greatest exposure, the very nature and selection of endpoints is expanding. Strong security requires more safeguards at the desktop, laptop, tablet, smartphone and more, including multi-factor authentication, encryption, and more.
- **Perimeter Control –** Cyberattackers often spend months finding the best way to exploit your network. Properly monitored, these attackers can be detected and very effectively blocked. Synoptek Active Watch and Security Log Management are just two of the powerful tools in our arsenal meant to patrol and protect your borders.
- **Firewall Management –** Since the function of a firewall is to enforce business rules that determine who and what can or cannot enter your network, our firewall services begin with the establishment and development of your data security policy. We then mount this policy onto your firewalls and assure that your rules are strictly and constantly enforced.
- **Web Filtering –** With organizations responsible for what their employees and others are exposed to online, our web filtering services become more important than ever before. We help you actively determine and enforce what sites are and are not available on your network at all times.
- **Security Incident & Event Management (SIEM) –** Detecting attacks is just the first step. What actions you take, what you do in event of an attack is even more important. Some regulatory acts carefully specify how you must report breaches, but even if you're not subject to those, having a clear action plan to manage your response to any anomaly or attack is crucial. Synoptek SIEM solutions assure swift, decisive action.
- **Anomaly Detection –** Many organizations have discovered, all too late, that the majority of network breaches may indeed come from within. The best way to protect against internal and external attacks is to monitor behaviors on your network and identify those that are unusual, anomalous, unexpected. Often, investigating these leads directly to bad-actors within the enterprise as well as without.
- **Virtual CISO –** Every company would benefit from having a Chief Information Security Officer (CISO) on their team, but many cannot budget for it. Now they can! Consistent with the shared resources strategy that enables cloud computing, Synoptek security experts are available to become a virtual component of your management team. As a virtual resource, you pay only for what you use. As a Synoptek specialist, you know they have the expertise and experience you need to enhance your security profile.

Synoptek Managed IT Security Services are designed to be modular so that a program can be specifically tailored to suit your organization's needs. Talk with a Synoptek Security Specialist to learn how we protect your most valuable data assets without busting your budget.

Synoptek

888.796.6783
Synoptek.com