NFINIT

Corporate Cyber Security:

Threats and Solutions
You Need to Know

For millennia, the primary way that humans defended their livelihood from foreign threats involved banding together and constructing protective fortifications around them; castles, walls, gates, moats, towers, and sentinels all played an incredibly effective role in repelling or dissuading hostile intrusions. But now, such castle defenses are relics of older age — made obsolete by changes in technology.

Today, in the Information Age, the invasive forces that businesses must now repel have changed from hordes of barbarians to criminal groups of digital hackers. So, while your physical safety may no longer be in jeopardy, the potential dangers that your business faces are just as serious. In fact, they’re more sinister, since the enemy is faceless, nameless, and capable of desolating an unsuspecting business remotely with but a few strokes of the keyboard.

All too often, IT departments — the people on the front line of the cyber war — report that they feel outgunned and outmanned by cyber criminals. As such, if you wish to protect your business, it’s vital that you thoroughly invest the resources to prepare for this ever-evolving cyber security threat. To that end, below, we’ll highlight and discuss common cyber risks, problems, and solutions so that you can take the proper measures to bolster your corporate cyber security.

The Importance of Cyber Security

Cyber security is a combination of processes, practices, and technologies that are implemented to protect the following from attack, damage, or unauthorized access:

Networks

Data

Devices

Programs

Today, just about every entity, whether governmental, corporate, financial, medical or military, will collect and store vast accounts of data — a large swath of which contains sensitive information such as personal information, financial data, and intellectual property. The goal of any cyber security system is to ensure that this data can be collected, disseminated, and stored without strangers being able to intercept it.

As such, a system will have to account for all of the following categories:

- Application security
- Business continuity planning
- Cloud security
- Data security
- Database and infrastructure security
- Disaster recovery
- End-user education
- Endpoint security
- Identity management
- Mobile security
- Network security

The Cyber Threat All Businesses Face

When businesses are asked why they don't take their cyber security more seriously, most will admit two things:

- They know little about the complex issue and begin to feel overwhelmed the more they hear about it.
- They assume a digital attack won't happen to them.

The second excuse is an especially common response for small to mid-sized businesses who operate under the false assumptions that they're not prime targets and they don't have that much to lose.

They couldn't be more wrong.

A 2019 State of Cybersecurity analytics report discovered that **66%** of small-to mid-sized businesses (SMB), had experienced a cyber-attack and data breach in the last year, a **7% increase** from 2017 reports. The cost of such breaches was substantial:

In the aftermath of these incidents, the respondents' companies spent an average of $1.43 million, a **33 percent increase** from $1.03 million in 2017, because of the damage or theft of IT assets. In addition, disruption to normal operations cost an average of $1.56 million, a **25 percent increase** from $1.21 million in 2017.

Even then, the monetary losses don’t paint a complete picture of the potential risks run by a company that’s derelict in its cybersecurity. These include:

Private Data Theft

Businesses store and use vast quantities of data including personal information, account details, and market information. When an attack happens, this data can be stolen, hurting both the customers and the company’s ability to operate in a reliable manner.

Hidden costs

On top of upfront expenses, there are a variety of hidden costs that can decimate a business and continue to impact it for years down the line. This includes both the time and money costs of fraud, embezzlement, restoring lost data, forensic investigation, post-attack disruption to business, buying new software, and training new IT.

Diminished client trust

Customer trust and satisfaction are the lifeblood of any business. Few things can sour a customer as quickly as hearing that their personal information has been stolen due to a favored-business’ supposed negligence. Once that trust is gone, they will likely take their business elsewhere.

These are but a few of the reasons you need to take your corporate cybersecurity extremely seriously. **Remember that your business, whether small or large, is always vulnerable to cyber threats.** Therefore, if you wish to keep your business safe, you must take prudent action and operate as if you’re constantly under attack.

Simply put, the cost of inaction is far higher than the cost of overreaction.

The Shifting Corporate Threat Landscape

According to Sophos
there are **480,000 variants** of malware every single day.

The cybercrime landscape, which is expected to surpass **$6 trillion in annual costs by 2021**, is evolving daily; it’s constantly shifting and progressing in response to new threats or novel solutions to such threats.

As hackers become more sophisticated, so do IT departments. Naturally, this creates a cycle where both sides must unceasingly seek out new methods of attack and defense, which is why it’s such a monumental challenge that every business must embrace.

Cybersecurity Ventures had this to say on the matter:

> Cyberattacks are the fastest growing crime in the U.S., and they are increasing in size, sophistication, and cost. The Yahoo hack was recently recalculated to have affected 3 billion user accounts, and the Equifax breach in 2017 — with 145.5 million customers affected — exceeds the largest publicly disclosed breaches ever reported. These major hacks alongside the WannaCry and NotPetya cyberattacks which occurred in 2017 are not only larger scale and more complex than previous attacks, but they are a sign of the times.

Every day, the internet and the amount of data on it grows exponentially larger. As a result, if you want to have the best corporate cyber defense possible, your workers, IT department, and security systems have to work in harmony to accomplish three tasks:

- Mitigate risks and prevent attackers from infiltrating your system.
- Learn new and/or unique techniques to gather exploitation intelligence, identify risk, and demonstrate impact.
- Search for ways that your team can internally identify, defend, and counter security threats.

To help you with that end, below you'll find the most common cybersecurity threats as well as potential solutions to those problems.

Common Cybersecurity Threats

It is very common that you and your IT team will run into most (if not all) of these potential issues. Knowing what they are, how to identify them, and how to counter them could be the factor that saves your business. They include:

Your Employees

Employee negligence is widely considered to be the number one threat to US businesses' security. Security Magazine had this to say:

> Employees are still falling victim to social attacks. Financial pretexting and phishing represent 98 percent of social incidents and 93 percent of all breaches investigated – with email continuing to be the main entry point (96 percent of cases). Companies are nearly three times more likely to get breached by social attacks than via actual vulnerabilities, emphasizing the need for ongoing employee cybersecurity education.

While some of these user errors are intentional, the vast majority are simply the results of employees making uneducated decisions like falling for a phishing attempt or going to a website that has malware.

Steps you can take to minimize such user errors include:

Cybersecurity education

An employee who's been trained to see the signs and risks is much less likely to fall prey to an obvious cyber threat. Take the time to educate your employees about common threats and to train them to spot red flags.

Set a policy of least privilege

Limit which employees have access to which files, devices, and resources in order to reduce the impact of any breach that might occur. By setting confines, you give fewer people access to sensitive data, which leaves it less vulnerable to human error.

Set a Bring Your Own Device (BYOD) policy

Such policies set the standard for how employees can or can't use devices at work. Ideally, you want to avoid allowing unprotected personal devices that may be compromised from gaining access to your networks.

Phishing

Phishing attacks are targeted digital messages, such as an email, which attempt to fool users into clicking on the provided link or providing personal information. Doing so allows the device to install malware or reveal sensitive data.

Common phishing scams include:

- Embedding a link in an email that redirects to an unsecure space
- Installing a Trojan in a malicious email attachment
- Pretending to be a reputable email source and requesting sensitive information.

The final method is how Capital One faced a massive data breach in late July, 2019, when a hacker accessed the information of over 100 million Americans and 6 million Canadians who applied for credit cards dating back to 2005. Bank numbers and Social Security numbers were compromised for roughly 140,0000 U.S. credit card customers and about 80,000 secured credit card customers who had their linked bank account numbers accessed.

Phishing attacks commonly involve two particular threats:

Malware

A piece of software that is often included in phishing attacks. Malware is disguised to look like legitimate software but secretly carries out more sinister purposes such as spying on the system, stealing data, or manipulating a system's codes.

Crypto-Jacking

Also often referred to as drive-by mining, crypto-jacking is becoming a more and more prevalent and dangerous cyber threat. It is the process of hijacking a user's computer through an embedded section of code that powers a user's computer towards mining cryptocurrency for the perpetrator's gain.

Ransomware

A form of malware that, upon being opened, locks down the system and then encrypts the device, rendering it inoperable. Ransomware is one of the most deadly and sophisticated threats today, particularly since it can lock down an entire server until the company pays a ransom to the hackers. Even if payments are made, there's little guarantee that hackers will give back control of the system.

In recent years, phishing attacks have grown more sophisticated since a good portion of employees are, in fact, aware of their threat. In response, hackers have employed machine learning to create and send more credible fake messages in the hopes that a user will open the digital door as it were.

Prevention methods include:

- Employee training
- Installing SPAM filters and antivirus software
- Updating all systems with current security patches
- Using a web filter that blocks malicious websites
- Encrypting sensitive company information

Mobile Security Threats

As people have shifted to using their mobile devices at an increasingly larger rate, hackers have sought to step up their game by tailoring phishing scams to mobile devices. In fact it has been said that mobile users are at the greatest risk of falling for it because of the way many mobile email clients display only a sender's name — making it especially easy to spoof messages and trick a person into thinking an email is from someone they know or trust.

IoT Attacks

The Internet of Things is a catchall term that represents the 30+ billion devices that interact with and connect to the internet. This includes:

- Computers
- Laptops
- Mobile phones
- Routers
- Smartwatches
- Webcams
- Smart systems

With each new cloud-computing device or IoT application that gets added to the system, hackers have increasingly more potential vulnerabilities to attack, particularly if the devices run on obsolete hardware or use out-of-date software. To make matters worse, companies are increasingly more reliant upon algorithms to interpret and apply their data, which leaves them vulnerable to algorithm manipulation, especially if they are not frequently monitored.

NFINIT Security - Responding to Cyber Threats

At NFINIT Technology Services, we take a “PPR” approach to your company’s cybersecurity. That is:

Proactive

We actively seek to create an overall corporate culture that values and understands security. Creating a culture of security awareness within an organization via user training, education, and awareness minimizes the most common security threat that any company will face — their own employees.

Preventative

We implement the right tools in order to thwart the vast majority of all attacks. For those that manage to get through the first line of defense, we install fallback systems intended to stop and mitigate issues before they can get out of hand.

Recovery

We help you plan for the worst-case scenario so that you can act decisively in the face of disaster. By having a recovery plan in place, we ensure that your business will continue to be up and running no matter what.

The NFINIT service stack provides support and consultation that’s intended to reduce your costs, increase compliance, and ensure your security systems are reliable.

In our decades of work, we know one thing is for certain — **cybersecurity isn’t static.**

It’s not simply a wall that you erect to hide behind, and hope for the best. Rather, those digital ramparts must be constantly secured by vigilant sentinels. Cracks in the wall or vulnerabilities must be addressed immediately lest they are used as an illicit means of entry.

In a world where the threats are multi-variable and unpredictable, you need a corporate security system that evolves with and responds to the changing perils.

If you want peace of mind about your cybersecurity system; if you’re ready to feel completely confident in your ability to protect your business and its vital information - you needn’t look any further.

At NFINIT, we’re here to help you map, implement, and monitor your complete cybersecurity program from A-Z, and will confidently grow alongside you as your company scales and innovates.

All you need to do to get started is to schedule a completely free consultation with one of our seasoned industry experts.

Have questions about cybersecurity or about your unique business needs? The answers await!

CONTACT US