CYBERCRIME DEFENSE GAME PLAN

A straightforward guide to defending your business

KLOUD9

TABLE OF CONTENTS

Introduction

Business owners and managers have a lot on their plates, from overseeing sales and marketing to managing human resources and finances. This is why some of them may overlook fortifying their company's security posture. Not having a robust cybersecurity infrastructure in place could easily become an extremely costly mistake that can result in their business's closure.

Doing business today requires making cybersecurity a priority, and this eBook will show you why this is so. You'll also learn the top cyberthreats you must watch out for and what concrete steps your business needs to take to keep them at bay.

Why it's important to boost your company's security posture

There are many reasons why businesses need to prioritize cybersecurity.

Heavy reliance on IT

Organizations today use IT solutions in each and every aspect of their operations, from marketing to accounting to customer service. For everything to run smoothly, these tools need to be operational at all times. Unfortunately, a single cyberattack can shut down IT systems, which can disrupt critical processes and cause businesses to lose their data. This can result in an expensive and time-consuming recovery process.

Growing threat of cybercrime

The threat of cybercrime is constantly growing. From 2014 to 2018, the number of security breaches reported around the globe increased by 67% and the cost of cybercrime rose by 72%.

More recent statistics mirror this growing trend, with the average number of cyberattacks per organization increasing by 31% from 2020 to 2021. Global cybercrime costs are also expected to increase by 15% every year for the next five years, translating to an annual cost of $10.5 trillion by 2025, up from $3 trillion in 2015.

Cybercriminals targeting all types of businesses

Gone are the days when only large enterprises had to worry about cybercrime. Today, cybercriminals are also going after small- and medium-sized businesses (SMBs). In fact, 43% of cyberattacks are aimed at small businesses and 66% of SMBs reported suffering a cyberattack in the past 12 months. Alarmingly, 60% of SMBs permanently close within six months of an attack.

So why do cybercriminals attack SMBs? For one, SMBs are often easier targets than large businesses. SMBs usually don't have the budget for top-notch cybersecurity solutions and experts, which results in weaker cyber defenses.

Additionally, SMBs can serve as a gateway to attacking larger enterprises they do business with. In fact, from 2020 to 2021, 51% of companies suffered a data breach caused by third parties, such as their vendor, supplier, or partner.

The top cyberthreats that businesses face

A great start to improving your company's security posture is learning about the most common cyberthreats making the rounds.

Social engineering attacks

Social engineering attacks are when cybercriminals use manipulation to trick victims into performing a desired action, such as wiring money or giving up sensitive information or access to systems.

Examples of social engineering attacks include:

- **Phishing** – Phishing attacks typically use email or text messages that appear to be from a legitimate source to get victims to click on a malicious link or attachment.
- **Pretexting** – This involves creating a false story or scenario to convince the victim to divulge sensitive information, such as login credentials or financial details.
- **Scareware** – A scareware attack uses pop-up messages or ads that appear to be from legitimate organizations to trick victims into clicking on a malicious link or downloading malware.
- **Baiting** – This commonly involves leaving a physical device or USB drive loaded with malware in a public area in hopes that someone will find and use it. If the device is plugged in, cybercriminals may gain access to the victim's system.

Ransomware attacks

In a ransomware attack, cybercriminals hold a victim’s data and computer systems hostage until the ransom is paid. However, paying the ransom does not guarantee the data's release. There have been cases where victims who paid the ransom did not get their data back or received corrupted files.

Ransomware attacks can be very costly, not just because of the money required to pay the ransom, but also because of the costs related to lost productivity and revenue. They can also disrupt or stop business operations and even lead to data loss.

Third-party exposure

Third-party exposure occurs when data shared by a business with a third party, such as a vendor or supplier, is leaked due to a hack on the third party's systems.

Insider threats

An insider threat can be an employee, a partner, a contractor, or anyone with legitimate access to a company's network. There are three types of insider threats:

- **Negligent insiders** – users and IT admins who inadvertently endanger the company by making mistakes, such as skipping software updates, using weak passwords, falling for online scams, and unintentionally divulging confidential data
- **Malicious insiders** – users and IT admins who intentionally cause harm to the organization in order to seek revenge, spy on business operations, or gain profit
- **Credential insiders** – cybercriminals who steal login credentials to gain access to company networks

Credential stuffing attacks

Credential stuffing is a type of attack where cybercriminals use stolen usernames and passwords — typically those exposed in a breach or sold in the dark web — to gain access to multiple accounts. They usually recruit an automated network of bots to log in to online services using the stolen credentials. If cybercriminals find a set of login credentials that work, they have complete access to the data stored within that account.

Such attacks are incredibly widespread because people tend to reuse passwords across multiple accounts.

Security misconfigurations

Security misconfigurations are weaknesses in systems and applications that can be exploited by cybercriminals. These weaknesses can be caused by errors in configuration, coding, or deployment.

Examples of security misconfigurations include:

- Not changing factory default passwords
- Failing to patch systems and applications
- Giving too much access to users
- Failing to limit access to sensitive data
- Allowing remote access without proper authentication
- Leaving servers and applications exposed to the public

Security misconfigurations are often the result of human error, but they can also be caused by poorly written code or default settings that weren't changed during deployment.

Cloud vulnerabilities

With the rise of remote and hybrid work arrangements, the use of cloud services has become even more popular among businesses. While the cloud offers a host of benefits, it also exposes businesses to security risks, such as:

- **Account hijacking** – A cybercriminal takes over an online account and uses it for malicious purposes, such as launching attacks or stealing sensitive data. Once an account has been hijacked, it can no longer be accessed by the owner.
- **Denial-of-service attacks** – A cybercriminal floods a server with requests, preventing it from processing legitimate requests. This can result in the temporary shutdown of a website or service.
- **Web app breaches** – Using various methods like embedding malicious codes in a poorly coded application, a cybercriminal gains unauthorized access to a web app and then steals sensitive data or launches attacks.

Creating an effective cyber defense strategy

An effective cyber defense plan involves the adoption of a defense in depth (DiD) strategy.

DiD involves implementing multiple layers of defense to protect systems and data from all types of cyberthreats. It integrates technology, people, and operational capabilities by leveraging three types of security controls: physical, technical, and administrative controls.

Taking these three steps will help you implement your DiD game plan successfully:

Step 1: Put in place physical controls

Safeguard your systems, facilities, and staff from physical threats, such as unauthorized access, theft, or damage, by doing the following:

- □ Keep IT equipment behind locked doors and in areas with video surveillance, sensors or alarms, and security guards.
- □ Require users to present their IDs, use keys, or scan their key cards, badges, or biometrics before giving them physical access to certain areas of your offices.
- □ Require visitors to prominently wear visitor IDs and have them escorted by a properly trained employee while they're on company premises.
- □ Maintain log forms of physical access.

Step 2: Deploy technical controls

Implement the following technical measures to control access to and usage of sensitive data and IT systems:

- □ Use a firewall to scan incoming and outgoing traffic between your company's internal network and the outside world based on a set of rules.
- □ Scan devices for malicious code using anti-malware software equipped with the latest threat intelligence databases and behavioral monitoring technology.
- □ Subscribe to spam protection to filter out malicious emails from inboxes.
- □ Encrypt company data so that it's converted into an unreadable format that can only be decoded using a decryption key, preventing unauthorized access to data.
- □ Use a password manager to securely store passwords.
- □ Require employees to use a virtual private network when working remotely to secure their connection to the company network.
- □ Leverage a mobile device management solution to secure and control mobile devices that have access to company data and IT resources.
- □ Deploy an identity and access management solution to manage user identities and specify who is allowed to access which systems and data.
- □ Enable multifactor authentication for all online accounts. This way, users will be required to present more than one proof of their identity (e.g., passwords, temporary SMS authentication code, fingerprints) before they're given access to systems or data.
- □ Implement an intrusion detection and prevention system to ensure round-the-clock monitoring, detection, and blocking of unusual network activities.
- □ Leverage a security information and event management solution. This tool collects and analyzes data from multiple sources to identify potential security issues before these issues disrupt business operations.

Step 3: Implement administrative controls

Your company must put in place policies, processes, procedures, and guidelines aimed at reducing the risk of a successful cyberattack.

- □ Create, implement, and regularly update security policies (e.g., remote work policy, bring your own device policy, and acceptable use policy) that all employees must follow.
- □ Educate employees about good cyber hygiene and teach them how to spot potential cyberthreats.
- □ Conduct thorough background checks on job applicants to safeguard the company from potential espionage or sabotage.
- □ When onboarding new hires, make sure to explain the company's security policies and procedures.
- □ Restrict employee access to systems and data based on job roles and responsibilities.
- □ Ensure that each user only has the bare minimum permissions necessary to perform their job.
- □ Disable the access privileges of employees who leave the company.
- □ Carefully examine the security measures of potential suppliers, partners, and other third parties before working with them.
- □ Regularly patch systems and software to mitigate any exploitable security vulnerabilities.
- □ Conduct penetration tests to identify vulnerabilities in systems and networks and create remediation plans.
- □ Create an incident response plan to quickly and effectively address security breaches.
- □ Regularly back up data to reduce the risk of data loss.
- □ Have disaster preparedness and recovery plans in place to ensure critical business operations can still be carried out even in the event of a major incident.

When physical, technical, and administrative controls are properly implemented, they can effectively safeguard businesses from even the newest, most sophisticated threats.

How Kloud9 can help

A successful cyberattack can hurt your business in many ways. It can disrupt operations, lower employee productivity, reduce sales, cause data loss, damage your reputation, and subject you to costly fines and legal battles. Fortunately, you can mitigate the risks of cybercrime by partnering with a managed IT services provider like Kloud9.

Our cybersecurity specialists at Kloud9 will conduct vulnerability assessments to identify weaknesses in your cyber defense and offer remedies to address these. We will also deploy and manage all the technical security solutions you need as well as guide you in crafting your company's security policies and procedures. Moreover, we will proactively manage your IT infrastructure and monitor your systems 24/7 to immediately detect and block potential threats.

Should your business experience a cyberattack, we will mitigate its impacts so you can quickly resume regular operations.

Let us help your business thrive amid an ever-evolving threat landscape.

CONTACT US TODAY!

Phone: **844- KLOUD9IT (5568394)** Email: **info@kloud9it.com**

KLOUD9

www.kloud9it.com