2021 Edition

Whitepaper

The Strategic Guide to IT Security

FROM DATA SECURITY FUNDAMENTALS TO THE LATEST CYBERSECURITY TRENDS

You depend on IT security to safeguard data and keep your business running. But your IT security perimeter is dynamic, and cybersecurity expertise is limited. A failure of IT security could result in a data breach or downtime. The success of your business depends on your IT security plan. You can minimize costly breaches and downtime with a well-designed IT security program.

What is IT Security?

Information Technology (IT) security is a strategy designed to protect the network, server, and application layers in an IT environment. It does this by stopping unwanted access to networks, computers, and data. Information security, a related term, refers to protecting the confidentiality, integrity, and availability of information (such as business-critical data).

Organizations large and small in the public and private sector implement security strategies to keep their businesses operational. The success of your business depends on your security plan and how it can prevent data security breaches and downtime. Working with an IT security services provider can help you plan for and limit the impact of internal and external threats to data, applications, and infrastructure.

What is Cybercrime?

The list of security risks and threats to your organization continues to grow. With cybercrime, malicious actors use tools such as malware, ransomware attacks, DDoS services, and hacking tools to infiltrate data sources. They often sell the stolen data on the dark web (also called the darknet). While their methods are constantly evolving, the aim of **cybersecurity** is to prevent intrusions caused by cyber-criminals.

In a landscape of evolving threats, IT teams face challenges that include:

- Serving remote workers, wherever they are
- Keeping organizations safe from cyber-criminals and insider threats
- Staying compliant with changing regulatory and compliance mandates

Proactive IT security takes many forms across multiple defensive layers, including:

- Cloud security
- Network security
- Application security
- Endpoint security

What is a Data Breach, and What Gets Stolen in One?

Whether your company's data is in the cloud or a traditional data center, it is a target for thieves supported by a thriving criminal ecosystem. **A data breach is an unauthorized intrusion into company data, usually associated with a cybercrime.**

The dark web provides a ready market for breached data, including personal health and financial data. Thieves are after any information that can be monetized, including corporate secrets and intellectual property.

According to IBM's *2020 Cost of a Data Breach Study*, the average cost of a data breach worldwide was $3.86M. The data most often stolen in breaches was personally identifiable information (PII) of customers. The biggest expenses in these breaches came from lost data cost - 39.4% of the total cost of a data breach.

Average Prices Paid for Stolen Credentials on the Darknet

$198.56
Access to a PayPal account

$15-35
Cloned credit cards with PIN

$65
Access to a bank account with a $2,000 balance

Preventing a costly data breach provides a substantial return on investment in cybersecurity. As a business, you have the responsibility to protect your client and employee data. Failing to do so can cost you money, clients, and trust.

Business Costs of Data Breaches

$6 trillion
projected in 2021

$10.5 trillion
projected by 2025

$135 billion
Projected global spending in 2022

$150
Individual cost per PII record (For 5,000 customers, that's $750,000)

$3.86 million
Average cost of a data breach

Types of Security Attacks

Even if cyber-thieves don't want your organization's data, your IP address and computing resources are targets. Hackers can hijack your computer systems and use them for cryptojacking, installing DDoS botnets, or spreading malware within your network and to others. Attacks could include:

- DDoS: An attack that overwhelms a network, website, or application with junk traffic.
- Cryptojacking: The unauthorized use of a computer or device to mine cryptocurrency
- Botnets: A zombie army of bots used for DDoS attacks, cryptominers, or spammers
- Web application attacks: A hacker exploits application vulnerabilities to gain a foothold in a network.
- Phishing: An actor attempts to gain information by imitating a trusted individual (spear phishing is a version of this where a specific individual is targeted).
- Ransomware: A criminal locks up data and demands payment to let it go.
- Insider threats: Threat comes from inside the organization from current or previously authorized users.

Read more: *Cybersecurity Attacks 101*
(https://www.tierpoint.com/blog/cybersecurity-attacks-101-phishing-cryptojacking-and-ransomware/)

How Do I Protect My Business From Security Threats?

Cyber-criminals change tactics constantly. A multilayered security approach is your best defense against next-generation threats.

7 Types of Physical Protection in Data Denters

Maintaining physical protection of your data can be just as important as cybersecurity. Physical threats can involve theft of hardware or attempts to sabotage a data center. Ways to mitigate physical threats in data centers include:

1. Checkpoints
2. Gates and fences
3. 24x7x365 on-site personnel
4. Badge/photo ID access
5. Biometric access screening
6. Secure cages
7. Full-building video capture

Establish a Cybersecurity Framework

The *National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)* is a popular structure of standards, guidelines, and best practices guiding strategy in organizations. The five actionable steps are:

1. **Identify** your most valuable and vulnerable workloads: mission-critical data, financial data, highly regulated data, etc.

2. **Protect** your valuable and vulnerable assets with tools such as multi-factor authentication (MFA), data loss prevention (DLP), next generation firewall NGFW), email protection, and more.

3. **Detect** incoming threats and attacks using tools such as intrusion detection systems (IDS), antivirus and anti-malware software, log management, and more. Focus on tools that monitor constantly and provide real-time protection.

4. **Respond** to threats. plan proactively and put a team in place as part of your disaster recovery and business continuity plans.

5. **Recover** your damaged capabilities and services. Minimize the financial impact on the business, repair lost confidence, and conduct a post-mortem to prevent it from happening again.

Developing an IT Security Policy

Organizations with an incident response (IR) plan can save *$2 million during a breach.* Developing an IT security policy helps you save money and shows your overall commitment to protecting your technology and data critical to your business functions and infrastructure.

An *IT security policy* is a critical part of a comprehensive strategy. Of course, a policy is nothing without effective implementation, which is best supported by a security-first culture. Mandating a foundation of security throughout the organization is one of the best ways to ensure your security policy is effective. Educating employees regularly, locking down workstations when not in use, and changing passwords regularly are a few things to include in a strong policy.

Fast Facts about Cybersecurity

95%

of cyberattacks are due to human error

88%

of organizations across the globe experienced attempts at spear phishing in 2019

96%

of data breaches were financially motivated, and 10% were motivated by espionage.

207 days

Average time to identify a data breach

78%

Attacks to supply chains increased by this much between 2017-2018

Choosing the Best Managed Security Service Provider (MSSP)

If you outsource some security functions to the right provider, you can:

- Ensure your cloud solutions are secure
- Improve your security posture with certified personnel
- Meet compliance mandates
- Improve the productivity of your employees
- Gain critical insight on the state of your security

Getting started on your journey to the right provider for your business doesn't need to be difficult. The right partner can help you achieve your goals and give you peace of mind. TierPoint's security services support your comprehensive strategy in three ways.

Customizing IT Security Solutions for You
TierPoint helps organizations like yours plan for and limit the impact of threats to data, applications, and infrastructure. Our IT security services let you customize your solution to safeguard each layer within your environment.

Enabling Digital Transformation
At TierPoint, we build our solutions around security, rather than the other way around. Our architects and engineers use a proactive, security-first approach that helps ensure your data is secure by design. We collaborate with you and customize solutions to help ensure protection for your data, applications, and infrastructure. We'll meet you where you are in your digital transformation journey.

Providing Responsive Partnership
TierPoint's customer-first mindset makes it a responsive partner in the planning, implementation, and maintenance of your solution. From planning to implementation and beyond, you'll get 24×7 support from our responsive experts.

tierpoint®

Improve Your Security Posture

Make sure you have the right mix of solutions
to secure your workloads and data.

Get Your Security Health Check

Call: 877.859.TIER (8437)
E-mail: sales@tierpoint.com
Visit: tierpoint.com

About TierPoint

A leading national provider of hybrid IT solutions, TierPoint helps organizations drive performance and manage risk. No U.S. provider comes close to matching TierPoint's unique combination of thousands of clients; more than 40 edge-capable data centers and 8 multitenant cloud pods coast to coast; and a comprehensive portfolio of cloud solutions, colocation, disaster recovery, security and other managed IT services. With white-glove customer service, TierPoint professionals customize and manage agile solutions that address each client's unique needs.