How to Think like a Hacker

and Secure Your Data

Introduction

There's no denying it: data security incidents are increasing. Organizations try to keep up with the latest cybersecurity best practices and technology, but the more they collect, process, and share large volumes of sensitive information, the more chances they have of getting hit by a cyber threat.

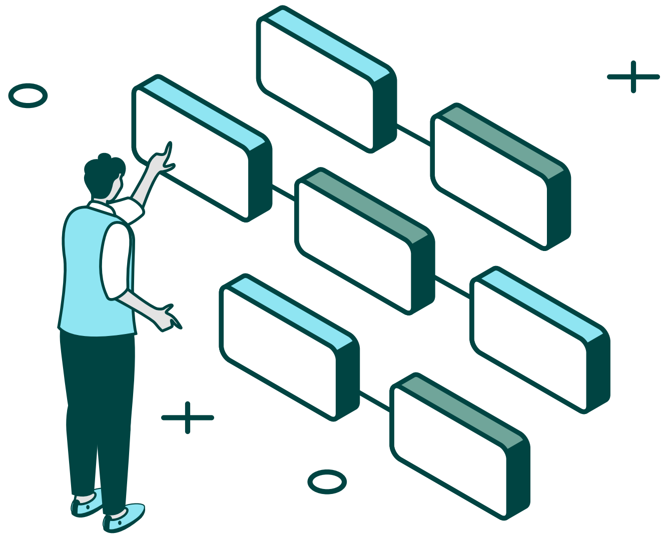
In response, IT teams play defensive. They create data breach response plans and security settings that tell them what to secure and how to react if those settings fail. But it's not enough to react to a security incident. Resources like response plans and guidelines can't predict what hackers are after or how they plan to acquire your data.

What if you looked at your cybersecurity from a different point of view?

In this guide, you'll learn how to go on offense with your data. You'll explore modern data breach statistics, walk through basic hacking terminology and techniques, dive into advanced persistent threats, and discover seven important strategies for protecting sensitive data.

Are you ready to put yourself in the shoes of a hacker? **Let's get started**.

Table Of Contents



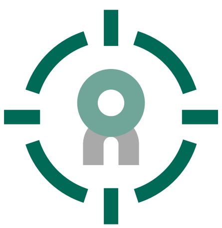
Modern Data Breach Statistics

Every year, organizations hope data breach statistics will improve. And every year, they're dismayed to discover that the cybersecurity tactics they're using to protect sensitive company data aren't foolproof. Hackers still manage to infiltrate their networks, using a blend of old techniques, new tactics, and human error to achieve success.

Getting ahead of cyberthreats can feel frustrating, but it's not impossible. The first step in making headway is to understand the lay of the land. To do that, let's start with a brief overview of today's data breach statistics.

Cause of Data Breaches

Most data breaches are caused by one (or more) of these issues:



Malicious/Insider Criminal Attack

Human Error

System Glitch

Modern Data Breach Statistics

Data Breaches Worldwide

According to Ponemon Institute in their 2019 Cost of a Data Breach Study, the average cost per record for all data breaches in 2018 was $148 as compared to $141 the year before. These costs often vary year to year, depending on who was breached and the money they paid after the breach to bolster their security.

Data breaches are not just limited to countries like the United States, Canada, and Germany, who continue to have the highest per capita costs. Smaller countries like Turkey, India, and Brazil also are affected, though they have smaller per capita costs.

Modern Data Breach Statistics

Cost vs. Frequency

According to the same Ponemon Institute study, the frequency of data breaches depends on the industry. Financial services, point-of-sale services, industrial manufacturing, technology, and retail are the five industries that experience data breaches most often.

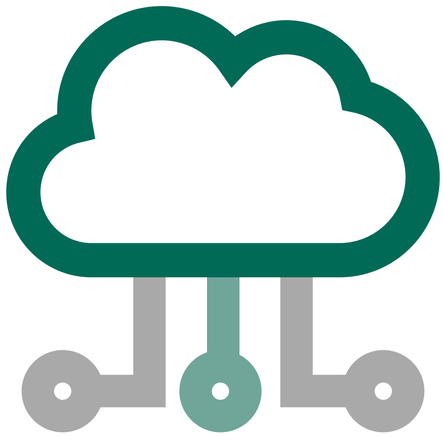
When it comes to cost, however, healthcare is the number one cost by industry. It doubles over financial services at $408 a record. Healthcare is particularly special because of the quality of each record stolen. Public health information (PHI) doesn't have a limited shelf life because, unlike credit card information or physical addresses/ emails, health records don't change.

Below healthcare, financial services, POS services, pharmaceuticals, and technology also have the highest price to pay, even if some of them are less frequently breached.

Third-Party Vendors & Cloud Migration

Third-party vendors, contractors, or other outside services used by a business tend to increase the cost of a data breach by $13 per record. The weaknesses they introduce to an organization can be anything from human error to accidental backdoor entries into the network.

Companies migrating to the cloud have seen a $12 increase in cost per record. Resolving a data breach during a cloud migration involves a lot of IT resources. Internal and external expertise are often needed, which explains the higher cost as people and technology are pulled in to address the issue.



Basic Terminology

The best way to think like a hacker is to understand the strategies they use to infiltrate an organization's network. It's also important to know some basic hacking terminology.

Here are the phrases most often used when discussing hacking and data breaches:

Reconnaissance: Most attacks start with some reconnaissance or due diligence. There are two types of reconnaissance that can be done days or months before the breach begins:

- Passive – Gathering information from Google, from WhoIs? domain names, from social media, etc. to collect data on employees that is publicly available. (For example, social media accounts may list where a person works, what their title is, and their contact info.) Passive reconnaissance can also include dumpster diving for letters, mail, and other credentials.
- Active – Gathering data that is not publicly available. This means interacting with the entity personally. It's invasive: a hacker will probe the network for hosts, IP addresses, and services. It can also be risky, as there's more chance of being detected.

Attack Surface: The threat vector or sum of all possible attack points. This is typically achieved after the reconnaissance stage when a hacker has knowledge of the devices that have been enumerated through initial probing. AKA: The landscape of where a hacker can attack a network.

Basic Terminology

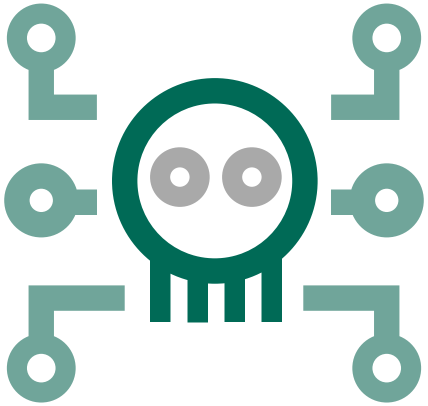
Attack Pivot: When a hacker targets a low security host (e.g., gets in through a phishing email) then uses that entry point to move laterally through the network and find areas with higher privileges. This escalates the attack to the real target: often people with access to sensitive information.

Attack Escalation: Ties into the attack pivot. Attack escalation is when a cyberattack evolves from low to high/critical value.

Critical Value Data (CVD): The prized organizational data, or crowned jewels, of an organization. CVD could be the secret ingredients in a popular recipe, proprietary formulas, or manufacturing processes.

Remote Access Trojan (RAT): A virus or malware that sneaks in with a legitimate program (often a phishing email) and opens a connection to an external command and control (C&C) device. One the RAT is in, it creates a remote back door for the C&C to use.

Command and Control: A device outside the target's internal network that sends commands to any compromised devices that have a RAT installed on them. Interesting or valuable data (the CVD) is exfiltrated back to the C&C as well.



Common Hacking Techniques

There are many techniques hackers use to get into an organization and steal records, but most attacks only need to use a few to be successful. Here are eight techniques you should know about:

Fake WAP

How it works:

A fake WAP (wireless access point) is put in a public spot. It usually has a legitimate naming convention to make it look like it's coming from a coffee shop or other trusted business.

A fake WAP is easy to set up and even easier to fall for. Once you're connected to a fake WAP, all traffic will traverse through a rogue access point for inspection. Any information that isn't encrypted will be sniffed by the hacker and potentially stolen for later use.

Key indicators of a fake WAP:

- It's an open, non-secure network
- No password is required to log in

How to avoid this technique:

- Don't connect to free open wireless networks
- Make sure you get the network name and password from the provider (for example, if you're at a hotel, ask for the network name to ensure you're using the right one)
- If you need to use a free network, use a host VPN to encrypt your traffic

Cookie Theft

How it works:

Cookie theft, also known as sidejacking or session hacking, happens when cookies from the websites you visit are stolen through an unsecure connection. The cookie can then be used to allow the hacker to pretend they are you. They can't necessarily gain access to your login credentials, but they can access the site as you (using your session ID) and change your account settings to hijack it.

How to avoid this technique:

- Make sure you're always visiting a secure site – https not http
- Use a host VPN to encrypt your traffic

Common Hacking Techniques

Bait and Switch

How it works:

The bait and switch hacking technique leverages internet clickable ads to divert a user to malicious websites. This largely depends on the advertiser who accepts ads: the larger the host site (like Facebook or Google), the more safeguards they have in place to prevent something this technique.

If a bait and switch is successful, the malicious site could either steal your credentials or install malware on your computer, which will help the hacker gain access to your computer and network.

How to avoid this technique:

- Don't click on ads while browsing the web – especially if it's solicited to you
- Use a secure browser plug-in that blocks pop-ups
- Use a browser or solution that recognizes known malicious sites

Clickjacking

How it works:

Clickjacking (also known as UI Redress) works by laying an invisible frame over the site you're on. This frame contains hidden buttons that often follow your mouse, meaning any click could be on that button. These clicks can help ads generate revenue or even unlock your camera and microphone.

How to avoid this technique:

- Use an up-to-date browser with built-in defenses
- Install plug-ins for adblocker and script blocking
- Use a solution that has a list of known clickjacking websites

Common Hacking Techniques

Browser Locker

How it works:

A browser locker is a pop-up window or screen with a message warning you about a virus, computer infection, or other incident. It encourages you to follow links that lead to malicious sites or phone numbers. On the other end of a call, a fake technician will attempt to have you pay for a fix or allow them to remote access into your computer to fix it themselves.

How to avoid this technique:

- Use a browser plug-in to block malicious links and ads
- Never call the numbers or click on the links provided
- If you aren't sure if the pop-up is legitimate, contact the company separately

IoT Attacks

How it works:

The IoT is coming out with a lot of exciting new products and features, but the general public are often disconnected with the security risks new technologies pose. Passwords and user names are frequently left as default, meaning hackers can compromise things like home appliances.

For example, an AC, refrigerator, or TV can watch you via cameras in your house. Compromised devices can be used as bots and find other access points into the rest of your home network.

How to avoid this technique:

- Ensure the IoT device is secure
  – Change the default user name and password
  – Place it on a different VLAN if possible – don't leave it on the default
- Use strong encryption and a complex password/passphrase
- Keep your software updated
- Leverage multi-factor authentication on your devices

Common Hacking Techniques

Phishing

How it works:
Most people know what phishing emails are. They're scam emails that are created to trick you into clicking a link, downloading a file, or calling a phone number.

While some of these are obvious (e.g., an email from a prince requesting to transfer money into your bank account), hackers are increasingly using social engineering to create realistic scenarios—like a spoofed email from a "coworker" sending you a "link" to the cutest cat photos on the web.

Key indicators of a phishing email:

- Spelling errors or unsolicited links/phone numbers
- Users called by "technicians" – e.g., Microsoft, Apple, etc.
- Bank users emailed about an account error
- Spoofed email from C-level individual asking for sensitive information
- Email from a job applicant with a PDF "resume" attached

How to avoid this technique:

- Invest in a good employee training program
- Create and distribute best practices on how to deal with phishing emails
- Foster an open workplace so employees aren't afraid to admit if they've clicked a bad email

Read More:
7 Steps to Protect Yourself against Spear Phishing

Credential Reuse

How it works:
We know we're not supposed to reuse passwords across various sites, but we still do it—or use similar versions of those passwords. This is an easy way for hackers to infiltrate your data across multiple websites. If one breach is successful and your login information is hacked, attackers can follow up with other sites you might be on. (Remember: This data can also be sold on the dark web, so multiple individuals could have your email address, user name, and password information.)

How to avoid this technique:

- Don't use the same passwords across sites or applications
- Keep informed of what sites or companies have been breached
- Use a password vault application
- Leverage a password compromise website like https://haveibeenpwned.com to see if a website using your email has been hacked

What Is Advanced Persistent Threat?

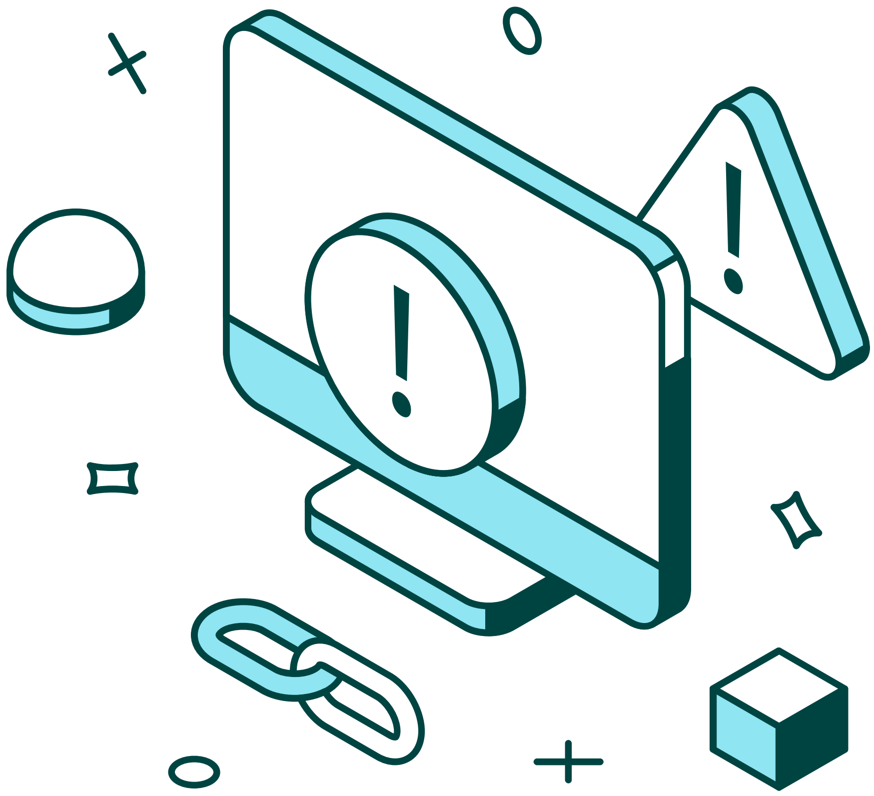
Advanced persistent threats (APT) are cyberattacks performed by nation-states and skilled hackers. They use multiple hacking methods (like the ones covered on previous pages) to infiltrate a specific target. The data they want to steal is often used in political espionage or for huge financial gain, and the attack is usually done over a long period of time.

There are six steps to an advanced persistent threat attack:

1. Start with reconnaissance
2. Gain access to the network
3. Probe the network
4. Establish multiple entry points
5. Gather target data
6. Exfiltrate data over weeks, months, or years

Advanced persistent threats have several key indicators:

- Elevated late-night logins
- Widespread backdoor trojans
- Unexpected information flows
- Unexpected data bundles
- Focused spear phishing campaigns



Seven Strategies For Data Protection

Now that you know the strategies hackers use to breach a network and steal sensitive data, what can you do to avoid these vulnerabilities and protect your information?

Here are seven tactics we recommend implementing today to boost your cybersecurity:

1 Get your C-level suite on board with cybersecurity plans.

Having support from the top (CEOs, CIOs, CISOs, etc.) will help ensure IT and security teams have the funding and resources they need to implement and maintain strong cybersecurity strategies across the organization. Without this support, it can be hard to get the infrastructure you need in place.

Related Reading:
How to Create a Cybersecurity Policy for Your Organization

2 Download your CIS top 20 controls.

Pull your CIS top 20 controls down and take an unbiased look at your network. This is a good starting point and will direct you toward the areas that need improvement. Having support from the top (CEOs, CIOs, CISOs, etc.) will help ensure IT and security teams have the funding and resources they need to implement and maintain strong cybersecurity strategies across the organization. Without this support, it can be hard to get the infrastructure you need in place.

3 Encrypt your data in transfer and at rest.

Encrypting every sensitive file, no matter if it's in transit to a recipient or stored on a server, should be one of the most important practices in your cybersecurity arsenal, and for good reason: it's your last line of defense.

If you haven't yet, consider building a strategy that will encrypt your files and file transfers. Some IT teams use free Open PGP tools to achieve file security. Others opt for a centralized managed file transfer solution to protect their data. What you choose is entirely up to you and your business needs.

4 Identify your CVDs.

Take a risk-based management approach to your critical value data.

Seven Strategies For Data Protection

5 Evaluate any contractors, BAs, or vendors you're using.

Vet your supply chain. Are they following cybersecurity best practices when it comes to your data? It's also worth checking on credentials here to ensure outside parties only have access to the information they need to complete their job, and no more than that.

6 Create a data breach and incident response plan to follow in the event of an emergency.

Though the goal for most organizations is total breach prevention, some industry reports claim the question isn't "if" you'll be data breached. It's "when."

Thankfully, that doesn't mean you're doomed to pay massive fines and lose data. With a solid cybersecurity plan and incident response plan in place, a compromised system can be dealt with quickly, efficiently, and cleanly before things have the chance to escalate.

Ready to get started? We've compiled a list of this year's best templates and resources for building a response plan in this article: Data Breach and Incident Response Plans

7 Educate your employees on good cybersecurity hygiene and behavior.

According to a recent Verizon study, over 90% of successful malware attacks are due to employees opening phishing emails at work. These scams are proving to be a successful way of breaching organizations worldwide, and remember: it only takes one person to create a problem.

Invest in your employees. Educate them, teach them good security hygiene, and show them how to use these practices at work and at home. If they see how cybersecurity risks can affect their daily life and job responsibilities, they will be empowered to help the organization succeed.

Related Reading:

The Benefits of Empowered Employees: Why a Good Security Awareness Program Matters

About GoAnywhere

Paired with the right cybersecurity strategies, taking an actionable approach to securing your data can help you avoid the major risks and security pitfalls other businesses often fall into.

Get ahead of your IT challenges. Finally.
Need better cybersecurity tools to streamline compliance, data encryption, and other cybersecurity processes in your network? Fortra puts the power back in the hands of IT professionals with solutions that guard against the unexpected and optimize the routine.

GoAnywhere MFT is a secure managed file transfer solution that automates and protects your data exchange via an intuitive, browser-based interface. With a variety of useful features and modules, implementing GoAnywhere in your organization can help you meet compliance requirements for file transfers, increase your cybersecurity practices, and improve your workflows.

Learn more about GoAnywhere:
www.goanywhere.com/solutions/managed-file-transfer
Fortra also offers an array of cybersecurity solutions, including ones for virus protection, identity and access management, security and integrity monitoring, security policy management, and intrusion prevention and detection.

Check out our cybersecurity suite:
www.fortra.com/solutions/cybersecurity

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.