FIVE STEPS TO STRONGER SECURITY

HOW TO CONDUCT YOUR OWN INTERNAL SECURITY AUDIT

Protect your business against data breaches and other cybersecurity threats.

DASHLANE

This mini-guide explains why you should conduct an internal security audit and walks you through how to run one for your business.

All in five steps.

01 Assess your assets

02 Identify threats

03 Evaluate current security

04 Assign risk scores

05 Build your plan

What's the difference between an internal and external audit?

Learn the pros and cons of each method in the chart to the right.

Keep in mind that if you choose to do an internal security audit, it's important to learn the compliance requirements necessary to uphold security protocols in your industry. Once familiar, you'll know what to keep an eye on—and you can start on the first step of your internal audit.

INTERNAL AUDIT

Inexpensive for both small and large businesses

Less disruptive to internal workflows

Smaller, more nimble process that gets done more quickly

Can establish a consistent process and baseline for future audits

Because of the low cost and efficiency, can be done more frequently

May have a steeper learning curve for teams performing their first audit

Process could be affected by internal biases when evaluating own team's performance

Not always compliant with legal requirements, such as the Gramm-Leach-Bliley Act

EXTERNAL AUDIT

Prohibitively expensive for smaller businesses (hovering around $50k)

Requires coordination between internal and external teams, which can disrupt workflow

May take a longer time to both find a respected and affordable audit partner and for the partner to complete the audit

Because of the high cost and time requirement, cannot be done very frequently

May not be a consistent process if the audit partner changes

Performed by trained, seasoned professionals who have the appropriate tools and software

No biases when evaluating current security standards

Compliant with legal requirements, such as the Gramm-Leach-Bliley Act

Your first job as an auditor is to define the scope of your audit by writing down a list of all your assets.

It's unlikely that you'll be able to audit all your assets—so the final part of this step is determining which assets you'll audit and which you won't.

Here are some examples of assets:

Computer and tech equipment

Sensitive company and customer data

Important internal documentation

Next, look at the assets you plan to audit and list the potential threats next to each one.

Here is a list of common threats to consider:

Level of employee diligence

Your employees are your first line of defense—will they recognize suspicious activity (like phishing) and follow the security protocols laid out by your team?

Physical breach or natural disaster

While unlikely, the consequences of one or both of these things can be incredibly expensive.

BYOD (Bring your own device)

The shift to remote and distributed work has also created a rise in work done on personal devices and vice versa. Unless your organization prohibits BYOD, you should assume employees have access to company accounts on personal phones and computers. Any device that has access to your systems needs to be accounted for, even if it's not owned by your business.

Phishing attacks

Hackers and bad actors are increasingly turning to phishing scams to gain access to sensitive information. In 2020, 74% of U.S. organizations said they experienced a successful phishing attack.

Malicious insiders

It's possible that someone within your business or a third party with access to your data could steal or misuse sensitive information.

Malware

This accounts for a number of different threats, like worms, Trojan horses, spyware, and includes an increasingly popular threat: ransomware.

Poor password habits

Weak, stolen, or reused employee passwords are the #1 cause of data breaches. Find out why passwords are the weak link in your company security in our white paper "Password Management 101."

DDoS attacks

A distributed denial-of-service (DDoS) attack is what happens when multiple systems flood a targeted system (typically a web server) and overload it, thus rendering it useless.

Threat noun /THret/

Any activity, occasion, behavior, or thing that can cost your business a significant amount of money

It’s time for some honesty. Now that you have your list of threats, you need to be candid about your company’s ability to defend against them.

It is critical to evaluate your performance—and the performance of your department at large—with as much objectivity as possible.

For example, maybe your team is particularly good at monitoring your network and detecting threats, but it’s been a while since you had a training for your employees. You’ll want to consider how you can build a strong culture of security among all your employees—not just in the IT department.

Step 4 | Assign risk scores

Prioritizing the threats you've identified in this audit is one of the most important steps—so how do you do it? Assign risk scores and rank threats accordingly.

How to calculate a risk score

A simple formula for determining risk considers three main factors: potential damage from an event, likelihood of that event, and current ability to handle that event (determined in step three). The average of these three factors will give you a risk score.

Below is an example that designates a score of 1-10 for each individual factor. You and your team can use as many or as few factors as you deem necessary—and add weight to them accordingly.

RISK SCORE FORMULA

Potential damage + Event likelihood + Current security abilities /3 = Risk score

EXAMPLE ASSESSMENT: HURRICANE HITTING A COMPANY'S SERVER CENTER

All the servers for the business could lose power		The location of the servers hasn't experienced a huge storm in four years		You don't yet have a contingency plan for failing servers		Total risk score
10	+	3	+	8	/3 =	7

Other factors to consider

Current cybersecurity trends: What is the current method of choice for hackers? What threats are growing in popularity and which are becoming less frequent? Learn cybersecurity predictions and observations from a white hat hacker herself.

Industry-level trends: What types of breaches are the most prevalent in your industry?

Regulation and compliance: Are you a public or private company? What kind of data do you handle? Does your organization store and/or transmit sensitive financial or personal information? Who has access to what systems? The answers to these questions will have implications on the risk score you are assigning to certain threats and the value you are placing on particular assets.

Get news of the latest data breaches and learn how to respond today.

And finally, for each threat on your prioritized list, determine a corresponding action to take.

Eliminate the threat where you can, and mitigate and minimize everywhere else.
You can think of this as a to-do list for the coming weeks and months.

Not sure where to start?

Here are some common security solutions for you to consider.

Employee education and awareness

More than 80% of all hacking-related data breaches involve the use of stolen credentials or passwords. Employees are the weakest link in your network security—run training for new and seasoned employees to create awareness around security best practices, like how to spot a phishing email.

Email protection

Phishing attacks are increasingly popular nowadays—and they are becoming more difficult to identify. Once clicked, a phishing email gives a perpetrator several options for gaining access to your data via software installation. Consider spam filters and visibly tagging emails as internal or external to your network.

Password safety and access management

Invest in a business password manager to help eliminate password reuse, enhance password complexity, and enable secure password sharing. As the admin, you can easily manage and monitor employee access. If your company uses single sign-on (SSO) for certain key accounts, you can integrate your password manager with your SSO provider for simple and secure access.

Network monitoring

Consider network monitoring software to help alert you to any questionable activity or unknown access attempts. Software systems, like Darktrace, offer 24/7 protection and use artificial intelligence to help identify cybercrimes before they occur—though these systems are typically on the expensive side.

Data backup

Back up your data consistently to ensure that it's safe and separate in case of a malware attack or a physical attack to your primary servers.

Software updates

To secure access points, it's important for everyone on your network to have the latest software. You can enforce software updates manually, or you can use a tool like Duo to keep your sensitive accounts locked to employees whose software isn't up to date.

Security audit?
Check.

Congrats. You just completed your first internal security audit.

This should be used as a baseline for future audits, so you can measure your improvements (or areas that need improvement) over time. Creating an atmosphere of security awareness starts with you. And conducting a security audit was a crucial first step.

Ready to start implementing better security with a password manager?

Read "A Practical Guide to Cybersecurity with a Password Manager" to learn how to prevent risks and take more proactive measures.

Read the guide →