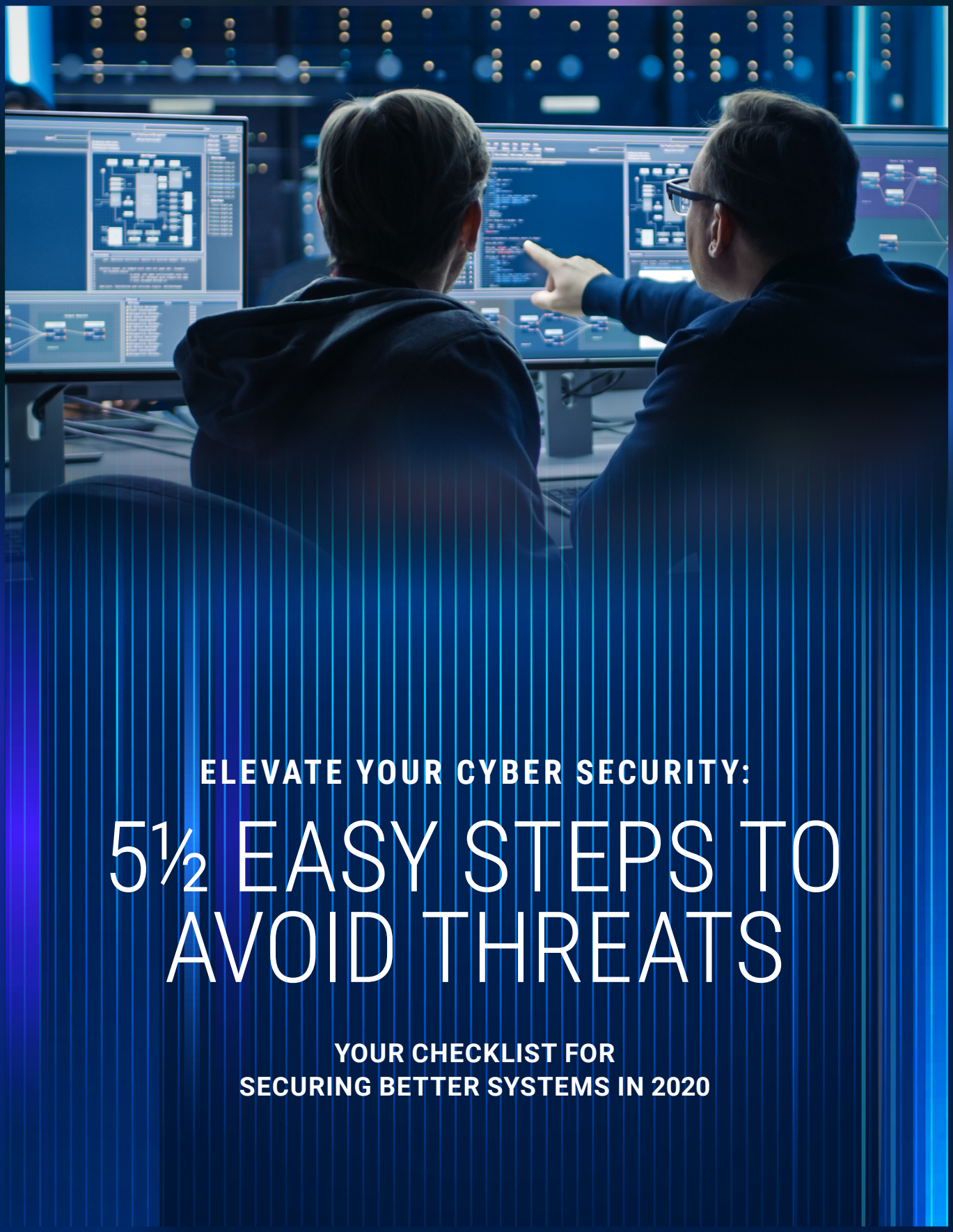

ELEVATE YOUR CYBER SECURITY:

5½ EASY STEPS TO AVOID THREATS

YOUR CHECKLIST FOR SECURING BETTER SYSTEMS IN 2020

mitnicksecurity
Kevin Mitnick and the Global Ghost Team™

Contents

Make 2020 the Year to Better Enforce Your Security

You're always looking for new ways to protect your business from hackers, but security best practices are constantly evolving— and it's hard to keep up with the latest cyber threats.

New breaches hit the news regularly, proving that even major enterprises aren't safe; in fact, these leaders are the prime targets for cyber criminals, eagerly after the wealth of data they possess behind digital doors.

We all know the business implications and cost of exposed data. Hefty penalties for breaking compliance and damaging reputation repressions are just the start— but even those are enough to set most companies back. For some, legal costs and PR blunders alone put them out of business.

What if you could drastically mitigate your threats in 2020? With the help of this guide, make the seemingly impossible task of safeguarding your business all-too possible.

This checklist is packed with professional guidance from the world's leading authority on security, social engineering and security awareness training: Kevin Mitnick and his Global Ghost Team.

Here are 5 (and a half) steps to avoid cyber threats and keep your company secure.

1. Train Your Team

The very first step you can take this year to mitigate your risk of data breach is to educate your employees and internal network on the latest social engineering tactics.

Cyber criminals often use employees as a gateway into your organization because they know your untrained, often not technically-skilled workers, are an easy way in.

Why are your employees such easy targets? Cyber criminals have clever ways of posing as authoritative figures, scaring your staff into taking action— like opening a malware-infected attachment or transfering money— for fear of repercussions.

These sneaky bad actors instill a sense of urgency or desperation to deceive unknowing employees into sharing data, money or access to private information with someone they think they can trust.

"Recent data breach statistics found that 63% of successful attacks come from internal sources, either control, errors, or fraud."

Here are three quick ways to educate your employees on the dangers of social engineering:

☐ Show Your Team Real Examples of Phishing Threats

Your staff may be aware of the concept of what a phishing email is, but could they identify a suspicious message if it arrived in their inbox? Give your team training on the common techniques used by malicious actors such as misspelled domain names, generic and informal greetings, urgent requests, and offers that seem too good to be true. Training your team on how to spot suspicious email addresses, links, and attachments can reduce human error and stop a phishing attempt in its tracks.

Forty-eight percent of malicious email attachments are office files, according to Symantec's latest report, so it's super important for employees to operate with caution

> A Security Awareness Training course like those produced by Kevin Mitnick and KnowBe4, use live video demonstrations to educate employees on social engineering red flags. These online classes show tangible examples and even walk your team through graded exercises to assess their alertness.

☐ Enact Organization-wide Password Protection

Easy-to-guess passwords are a quick way for bad guys to break into your systems. Scarily enough, modern password cracking software can unlock simple short, standard character passwords in a matter of minutes or even seconds.

In order to mitigate risk of having your users' passwords cracked, invest in an office-wide password manager, which can safely store logins behind encrypted doors.

> Watch how easy it is to crack a password with this demonstrations from Kevin Mitnick.

Even strong passwords can be stolen by a savvy hacker, who captures your keystrokes for your master password to your password management system. Consider implementing a multi-factor authentication system so that users must double verify to access sensitive information.

Despite using a gated password housing platform, strong password strength is always best practice.

A strong password policy configuration should adhere to the following properties:

- Recommends passphrase usage instead of a "standard" password. A passphrase utilizes multiple words in a sentence
- Contains upper and lowercase letters
- Contains numbers and symbols
- Contains spaces

Following these recommendations, you may choose to take the passphrase, "be the change that you wish to see in the world" and enhance it to read, "Be The Change That Y0u W!sh To See !n The W0rld." This replaces "I" characters with an exclamation point and "O" characters with zero.

☐ Ensure IT Staff Routinely Monitors Software & Application Updates

There's a reason there is an entire attack vector just for application review. Vulnerabilities within your applications can range from holes in design flaws and development to implementation and actual use.

When your IT team ignores updates, they leave holes in your security — missing patches or exploited gaps — that hackers use to get in. Verify that software updates and patches are included in your information technology team's policies and procedures and that they are strictly enforced.

> Hire an assessment team to run an annual Application Penetration Test. Because hacking tactics, techniques, and procedures evolve daily, it's important to frequently test your applications for new vulnerabilities— and to understand that automated scanners alone just don't cut it, as they usually only detect a small percentage of problems within the code base.

2. Create an Airtight Offboarding Process

Cyber threats don't always happen from the outside. Your employees handle a lot of sensitive data, and oftentimes have access to dozens of applications and platforms housing a wealth of information.

If a disgruntled employee leaves on bad terms and isn't offboarded properly, they could leak or steal private info, resulting in costly breaches or damaging reputational repercussions.

Even amicable departures can lead to breaches if tempting information is only a few clicks away.

Do you have a formal offboarding process for when an employee leaves, no matter if their exit was by choice or force?

Here are a few ways to create an airtight offboarding process:

☐ Revoke Access, Everywhere

Ensure your IT department immediately removes an ex employee's access to applications after leaving. Delete them as a contributor on any website interfaces, shared drives, social media management platforms, or anywhere that they have their own private login/account with access to your business's or your organizations's data.

☐ Change Commonly Known Passwords

If there's a password that your company uses for multiple logins, be sure to change it and avoid similar variations that could be easily guessed. Your best bet is to use a password management tool, which can save complex, hard-to-guess/remember logins reduce the risk of unauthorized remote access.

Flip back to page 5 for our recommendations for better password management practices or watch our video here.

☐ Shut Down Their Email

Your employee had their own company email under your employment, but old threads can easily be searched, copied, forwarded or saved. Upon leaving, immediately close your ex employee's email address, which can also prevent them from receiving password reset messages to try and change accessibility to accounts.

☐ Document & Communicate the Process

The whole point of formalizing a process is to ensure it's properly upheld and repeatable for future use. Build a list of checklist items to guarantee nothing runs amiss next time a staff member leaves.

☐ Don't Forget Your Vendors

When checking your partners' security, be sure to ask them about their offboarding process, and offer recommendations for hardening their exit steps to better protect your shared data assets. More on this in Step 4.

3. Stay Up-to-Date

In the same way that you should invest in employee training and continual cybersecurity education, you too should stay in-the-know about the latest threats and updates by subscribing to important cyber news outlets.

Because threats emerge so quickly, it may take some time for them to be implemented into a new cyber education curriculum and accepted as a new best practice. But by reading or listening to continual updates, you are amongst the first to know about evolutions in cybersecurity protection.

We look to the following trusted tech outlets for the most accurate cybersecurity news:

- Krebs on Security
- Troy Hunt
- ZDNet
- Business Insider
- Wired
- WSJ
- The Verge
- Vice/Motherboard
- CSO Online

WATCH OUT for sites that publish content from just about anyone, especially from authors/contributors without a background in cybersecurity or from authors who neglect to reference valid cybersecurity professionals.

For instance, while Forbes is an immensely popular news site, contributors are often not true editors or journalists. Other high-trafficked sources like Tech Crunch may also elicit contributors from all backgrounds, and should be considered with caution.

4. Consider Vendors & Partners

Many companies work closely with a variety of partners or vendors, all which share access to one another's data. A lot of this information is exchanged via cloud storage systems, and the touchpoints add up fast.

While you may be protected against cyber threats, your partners may have holes in their security that grant hackers access to your private data.

"The average company connects with 1,555 business partners via the cloud, including suppliers, distributors, vendors, and customers," according to research by McAfee.

In order to avoid external vendor-related cyber threats, be sure to:

☐ Organize Your Partners by Risk

Because most businesses have anywhere from a few hundred to a few thousand partner connections, it can seem overwhelming to check them all for vulnerabilities. Many companies perform initial security audits before signing onto a new partnership, but not all routinely evaluate their vendor regularly for changes to or holes in their protection.

If you haven't assessed your vendor's security since you began your partnership or in more than a year, it's time to review all connections this 2020.

To get started, silo your partners by connection: are they involved in the manufacturing side of things? Do they play a role in your PR or marketing? What about customer service? Do they provide software or a technology solution? By simply grouping them together, you can make a plan for analyzing them categorically.

From there, it helps to prioritize evaluating the security of partners who have the most access to your data by performing a vulnerability assessment. Then, request a recent security audit from your vendors and partners. Look at how recently the audit was conducted and how in-depth the report goes.

> Once you know who handles the largest portion of your data, you can better determine which vendor carries the most financial or reputational risk should they be breached— and organize your vendors by risk level.
>
> This will allow you to focus on your highest risk third-party vendors first. After learning about their potential vulnerabilities and threats, you can decide whether to accept, transfer, mitigate or avoid every potential risk with the help of a trusted consultant.

☐ Hire a Professional Team to Assess Your Vendor

If you don't have the funds or time to go through all of your vendors one-by-one this year, prioritize assessing your highest risk partners first.

Hire a professional assessment team to determine your associated risk with vulnerability and penetration testing exercises, specifically aimed at breaching your vendors' protective barriers.

An assessor will let you know if they were able to infiltrate your vendor's security measures and estimate a projected cost, should the incident have been real. They'll also be able to offer advice for mitigating your risk with the vendor moving forward.

> Choose a team of security professionals that takes a holistic approach to penetration testing. Ask what types of pentesting they perform, and ensure they have a wide offering, including both external and internal network testing, physical, wireless, externally facing web application, red team, mobile app review, hardware config review, social engineering and other methods for getting around your vendor's best defenses.

☐ Routinely Audit Partners

Penetration testing is not a once-and-done affair. Threat landscapes are constantly evolving, and in order to accurately understand each of your partners' security risks, you must perform consistent audits to analyze their security protocols.

The frequency of partner audits is contingent upon your industry. Banks and financial institutions, for instance, require a greater number of check-ins compared to a business selling consumer products. There is no one-size-fits-all answer for how often you should assess your partners, but a professional assessment team can offer individualized advice for your specific businesses' risk.

When assessing your partner, ask a few important questions:

- What security measures do you currently have in place?
- How are you protecting data exchanges, both between your business and the client and between your relationship with your separate vendors where you handle shared information?
- How do you check your security for holes and what steps are you currently taking to prevent breaches?

> It's impossible to say whether a vendor is objectively safe or not. Instead, it helps to establish metrics for tracking a formal security rating for each vendor on a given scale, and to develop risk monitoring strategies to stay up-to-date on all levels of risk.

☐ Limit Your Vendors' Access

In the end, the less information your partners have at their fingertips, the lower the risk of losing it in a breach. Prevent unnecessary exposure of sensitive information by restricting access to data your partners don't need.

> Establish restriction checks periodically to reevaluate your partners' level of access to sensitive information.

5. Hack Yourself

In the same way that we recommend hiring a cybersecurity expert to try and hack your vendors, we too suggest performing penetration tests on your own company.

☐ Hire A Professional Security Team

While you could run internal screenings to assess your security, these automated scanners are not thorough, often missing important gaps in your protection, and should be the bare minimum your internal security team already does as a part of your process and procedures.

A skilled pentester will attempt to gain access to your sensitive data, through any means necessary. These white hat hackers will target your firewalls and missing security patches, send employees malicious emails, simulate the access an ex employee might have and more to find holes in your security perimeter and beyond. They also look for misconfigurations on the cloud environment, perform password spraying techniques on their single sign on products (e.g like Okta), look for past data breach data on employees, OSINT research (Open Source Intelligence).

Once they find vulnerabilities, the right pentester will offer solutions for reducing your threat landscape, all broken down into easily understood, actionable steps.

5½. Don't Forget Pentesting for Physical Environments

Not all penetration testers stretch beyond your cyber risks, mistakenly honing in exclusively on your digital weaknesses. While, indeed, a large number of breaches are due to hacking or malware attacks, physical factors attribute to data theft or leaks too.

Criminals can break into your office space and steal equipment with sensitive information stored on it. Other bad actors are more mischievous, posing as delivery personnel to gain access to computers within your office or creating lookalike name badges to fool kind but unassuming employees. All it takes is for them to breach your physical environment and they have a doorway into your systems, too.

When searching for a penetration tester, be sure to ask if they perform physical pentesting too.

Are You As Prepared As You Think?

After reading through these few steps, are you discovering gaps within your security game plan for this year? Discover with certainty if you are secure by completing Mitnick Security's questionnaire— a quick 13-question assessment designed to instantly test your level of security.

These straightforward questions will walk you through some of these best practices and more to score your current risk and provide the next steps for you to take to keep your organization safe and secure today and in the future.

Take the Cyber Threat Assessment

About Kevin Mitnick and the Global Ghost Team

Formerly one of the FBI's Most Wanted, Kevin Mitnick earned his fame by hacking into 40 major corporations— just to prove he could. Today, he's a celebrity icon, global bestselling author and cybersecurity mastermind working on the other side of the law. His boutique security firm is one of the industry's most advanced, with a 100% success rate of hacking into client systems.

Know you're really protected against cyber threats with the help of a world-renowned penetration testing team, granting you unprecedented access into your hidden vulnerabilities.

Learn More About Partnering With the Mitnick Security Team

Contact Us