jumpGuide

ivp

# Protecting Your Company Online

by Zack Willis on behalf of IVP

## Security threats really are everywhere, all the time

Keeping your company safe is an endless but existentially important job. This jumpGuide includes best practices your company should adopt to prevent a security breach at an individual or organizational level. This guide, a companion to the **Protecting Your Employees Online** jumpGuide, is not comprehensive. However, implementing the items below will make your company a less conspicuous target for hackers and scammers online.

### Establish a relationship with government security agencies, such as the FBI and Homeland Security, or their UK or European counterparts

This may sound like a big step to take, but establishing a relationship with your relevant federal security agency is vital. That way, if you ever need to connect with them urgently (to report wire fraud, hacks, ransomware, etc.), you'll have an ongoing connection to rely on. Doing so also allows your company to get important intelligence and cyber updates directly from the agencies.

There are various ways of starting this relationship:

**In the U.S.**

- Calling your local FBI field office and asking to speak with an agent that deals with cyber/community outreach. Explain that you'd like to create an email relationship and check back every so often via email.
- Joining the FBI's InfraGard program. InfraGard is a partnership between the FBI and members of the private sector to protect U.S. critical infrastructure. InfraGard connects the FBI to critical infrastructure owners and operators to provide education, information sharing, networking and workshops on emerging technologies and threats. InfraGard members include business executives, entrepreneurs, lawyers, security personnel, military and government officials, IT professionals, academia and state and local law enforcement — all dedicated to contributing industry-specific insight and advancing national security.

- Join your local Fusion Center. Coordinated by Homeland Security and owned and operated by states, Fusion Centers serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information among State, Local, Tribal and Territorial (SLTT) agencies, federal agencies and private-sector partners.

**In Europe**

- In Germany, the Bundesamt für Sicherheit in der Informationstechnik (BSI) is the federal office for Information Security.
- In Britain, Action Fraud is the national reporting center for fraud and cybercrime. It works with the National Fraud Intelligence Bureau (NFIB), which is run by the City of London's police service.

---

## Get Cyber Insurance

Companies like Coalition include a wide range of services in their cyber insurance policies. They monitor your external resources for configuration issues and vulnerabilities, assist with incident response and provide a pathway to financial reimbursement when a qualified incident occurs.

## Create a incident response plan and set up an incident response retainer with a reputable cybersecurity firm

- Waiting until a breach occurs to establish a relationship with a cyber firm is not a winning strategy. Instead, set a retainer with a reputable company, to ensure support when you need it. Retainers are often expensive but can be used for other services if the money isn't needed for incident responses like penetration testing (pen testing) and red-team attack simulations. Companies like Mandiant and CrowdStrike offer these services.
- Create an incident response plan that includes a step for reaching out to your incident response firm, depending on the situation. ACA Aponix, Mandiant and many other firms can assist with writing your company's incident response plan.
- Test your incident response plan annually (at a minimum) by doing a tabletop exercise conducted, preferably, by a third party.

## Establish an (at least) annual employee cybersecurity training program

Your company's employees are, and always will be, the weakest link in security. Layers of security are good, but layered security with employee training is far superior. Training should be enlightening, interactive and compelling (it needs to be remembered). A good practice is to hold annual mandatory security training sessions with small groups of employees at a time. Phishing tests should be conducted at least quarterly as part of security training. Some ideas to make this a better experience for employees:

- Do something unique and memorable. For example, IVP had a catchy song commissioned that covered all the topics covered during security training. People sing it to this day.
- Offer rewards for security awareness. Gift cards are a great option and can be handed out for things like reporting a phishing email, reporting suspicious behavior and offering tips to other employees.
- Have your favorite celebrity deliver a powerful cybersecurity message using something like Cameo.
- Use real and relatable examples of cybersecurity incidents to drive the message home.
- Make it interactive. Don't wait until the end for questions. You want to encourage questions and dialog, so you can clarify things for your employees along the way.
- Teach your employees to slow down and ask themselves questions before acting. Is this email expected? Am I really at the website I think I'm at? How do I know this person is who they say they are? When in doubt, instruct them to reach out to security and make clear that you are there to help, always.
- Disseminate the **Protecting Your Employees Online** jumpGuide.

## Use a third party to conduct annual internal and external pen tests (penetration tests) and don't use the same vendor more than two years in a row

Find a reputable cybersecurity firm that can do an extensive internal and external pen test with more than just automated tools like Tenable. For a pen test to be successful, humans have to take action when incidents occur, to see if potential vulnerabilities are actually exploitable. This allows you to prioritize what needs to be fixed and provides a lot more information about your security posture than a tool like Tenable ever could. Pro tip: Change providers at least every 2 years, because auditors will become familiar with your environment and may miss things that a fresh set of eyes won't.

## Use automated internal and external pen testing tools on a monthly basis and after any change in your environment

- This is where a tool like Tenable comes into play. You can set scans to run however often you choose, but monthly is a great practice. After each scan, review the results and fix any issues it finds.
- New AI-based pen testing tools are also hitting the market. These tools not only find vulnerabilities, but also try to exploit them the way a real pen tester would. Once this market is established, the tools will be much more effective at helping you find, fix and verify security issues. Horizon3.ai is an example of this tech.

## Establish an aggressive patching program for all company devices

- Patching is essential to security. Use tools like Automox and Ninte to push out third-party updates in real time and schedule OS updates at least weekly.
- Don't forget about devices like uninterruptible power supplies, power distribution units and printers. Such devices are potentially full of security risks and are often overlooked for patching. Make an inventory, know the current OS version, and check for updates at least monthly.
- The easiest way to patch mobile devices is through Apple's device supervision program or Android's EMM program.

## Go passwordless

- Passwords, no matter how strong they are, can and will be compromised. A passwordless solution not only makes the lives of your employees easier but also can greatly improve your security. Solutions like Beyond Identity sit in front of your identity provider and help establish zero trust with robust policies that are enforced before authenticating.
- If your company isn't ready to go passwordless, your employees absolutely must use a password manager like 1Password with strict master password guidelines.

## Use 2FA or MFA for everything

- There are many solutions that  make using 2-Factor Authentication (2FA) or Multifactor Authentication (MFA) easy for your employees. One is Duo Security. If you can enable MFA for something, do it. Don't lapse into thinking that some apps or services are so inconsequential that you don't need to enable MFA for them. A hacker will find a way to exploit any unprotected parts of your network. NOTE: Passwordless providers like Beyond Identity have MFA built in. It's a seamless user experience, with no prompts or codes.

## Other steps to consider

- Harden your computers by turning off weak encryption methods, disabling services and following best practices
- Protect your remote/traveling employees by implementing an always-on VPN and a DNS filter like Cisco Umbrella
- Harden your mobile devices using Mobile Device Management (MDM) software such as Microsoft intune and Meraki
- Force Transport Layer Security on outbound emails
- Encrypt all devices
- Use an Endpoint Detection & Response system like CrowdStrike or SentinelOne
- Store logs from everything for at least a year (a Security Information and Event Management solution is a great option for this)
- Install honeypots — virtual traps that trick hackers — in your environment
- Test your alerting capabilities
- Test your incident response plan
- Create a messaging channel like Slack or Teams where your security team can share tips and information with all employees
- Host monthly lunch & learns where employees can talk with your security team, ask questions and get updates
- Offer employees tools like Optery, to remove their information from the internet and cut down on phishing, and SpyCloud, to notify them of any breaches of their personal or business email
- Do not give employees local admin rights to their computers — removing admin rights can stop many attacks

## Make security part of your company's culture

- This process is not easy. But it will happen over time if you take steps that include the recommendations offered above. The biggest hurdle is to get employees to understand why security matters and help them avoid the mindset of, "Our tech team is on it, so I don't have to worry about it."
- Employees should understand that their role in security is just as important as the tools used to protect the company.
- Just one compromised employee account can cause a breach that greatly damages your entire company's reputation.

## When should you hire a CISO?

This is not an easy question to answer. Each company must decide for itself when the time is right to bring in a CISO. You may hear things like, “Hire a CISO after you reach $50m in revenue … or 250 employees …” or other markers on your company's path to success. Those are fine measures to think about, but they aren't rules. Hiring a CISO is a critical step that should not be taken too late in your growth. CISOs have an incredible amount of responsibility and can truly change an organization. Not many will want to join your company right before an IPO, because the amount of work they will have to do to get the company ready will probably not be proportional to the payout they’d receive. Conversely, many CISOs won't want to join a company with only 10 employees, as there won't be anything for them to do. Things to consider:

- Your company's industry and regulations: How many regulations does your company need to comply with?
- Your customers: What kind of security are they demanding?
- Can you afford a CISO? They command high salaries, but a breach can be much more costly to your company.
- Is it a cultural fit? Have you already made security part of your company’s culture?
- Are you looking to get data-security certifications such as SOC2 and/or ISO 2700? A CISO can greatly help with the process. Either I, an IVP partner or someone from our network of CISOs can walk you through the process.

If you aren’t sure, start with a virtual CISO (an outside consultant) and transition to an in-house CISO when you both feel the time is right.

---

The quantity and quality of online security threats only grows with time. Enact the above online security recommendations now and not after your company has discovered a malicious breach. Such breaches could negatively impact your business’s operations, growth potential and reputation.

For questions about or feedback on these recommendations, please contact IT@ivp.com.

---