10 WAYS YOUR ENGINEERING FIRM IS AT RISK FROM HACKERS

WHY YOUR FIREWALL AND ANTIVIRUS ARE NOT ENOUGH

InhouseCIO

THE COST OF AN ATTACK

Cybercrime is at an all-time high, and hackers set their sights at “low hanging fruit” – small and midsized businesses. In fact, 71% of ransomware attacks were targeted at small and midsized businesses in 2018. Many CEOs and CFOs at companies this size consider themselves an unlikely target for cybercrime. They mistakenly think “I’m to small to be of interest to a hacker.” But they’re wrong. In fact, the hackers see them as easier targets than large companies who have whole teams of security experts working for them.

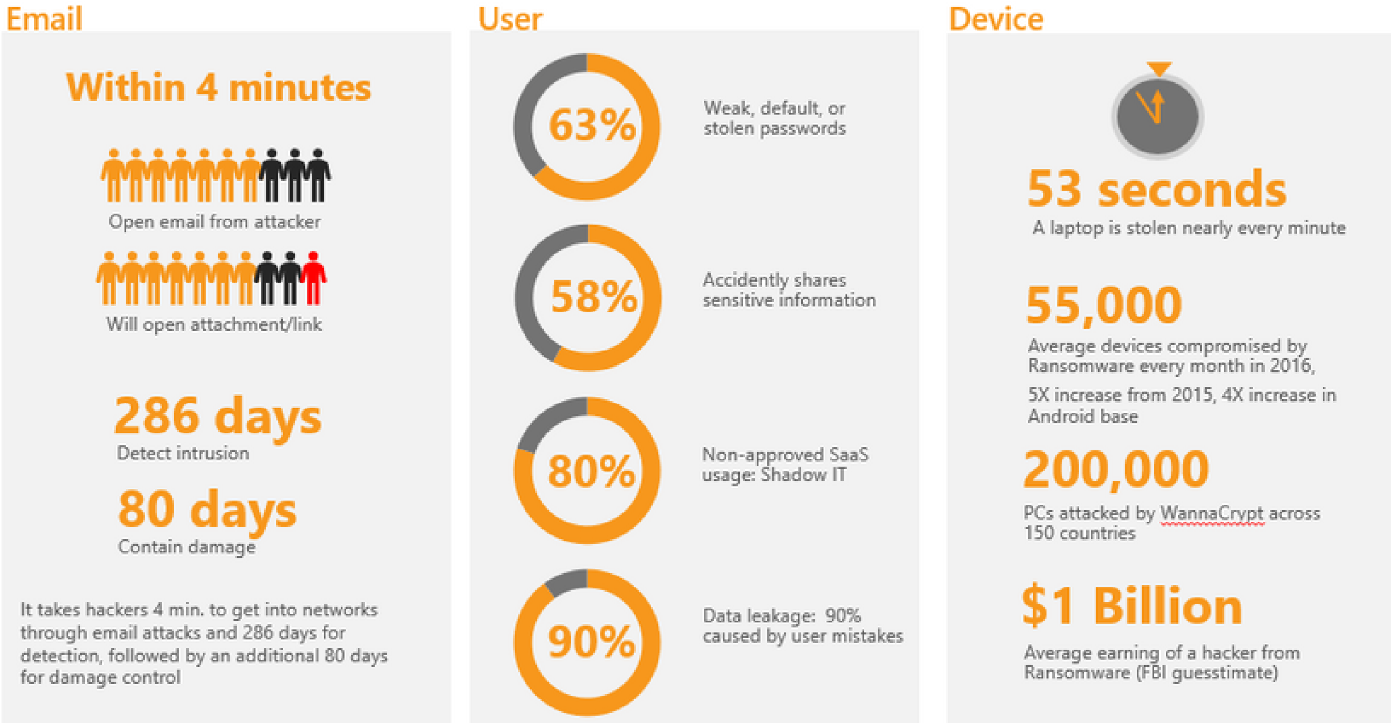
60% of SMBs will go out of business within 6 months of a cyberattack. The downtime it causes, the additional IT support required for recovery, the lost company assets or funds, the damage to reputation and decline in client confidence, and any litigation or legal costs all become too much for a small or midsized business to recover from.

Your engineering firm is not immune.

WHY YOUR FIREWALLS AND ANTIVIRUS FALL SHORT

The technology today's hackers are using are becoming more and more sophisticated. Not all hacks are the type that make the news. They hack into thousands of small businesses to steal credit cards, client information, tap into your bank accounts, or hold your networks and data for ransom.

The basic problem IT professionals face is they're still relying on traditional network defenses to guard against emergent threats that have been designed specifically to skirt them. You need to go beyond traditional firewall and antivirus solutions to protect your business in three key areas: email, your users, and your devices. These are the key areas where hackers get in.



Email

Within 4 minutes

Open email from attacker

Will open attachment/link

286 days
Detect intrusion

80 days
Contain damage

It takes hackers 4 min. to get into networks through email attacks and 286 days for detection, followed by an additional 80 days for damage control

User

63% Weak, default, or stolen passwords

58% Accidently shares sensitive information

80% Non-approved SaaS usage: Shadow IT

90% Data leakage: 90% caused by user mistakes

Device

53 seconds
A laptop is stolen nearly every minute

55,000
Average devices compromised by Ransomware every month in 2016, 5X increase from 2015, 4X increase in Android base

200,000
PCs attacked by WannaCrypt across 150 countries

$1 Billion
Average earning of a hacker from Ransomware (FBI guesstimate)

InhouseCIO

HOW HACKERS FIND THEIR WAY IN

There are ways to minimize your risk of falling victim to a hacker. Once you understand the risks every engineering firm faces, you can prioritize your ways to manage them. There is danger in complacency.

1. THEY TAKE ADVANTAGE OF POORLY TRAINED EMPLOYEES

The #1 vulnerability for business networks is the employees using them. Any employee can infect an entire network simply by opening and clicking a phishing e-mail cleverly designed to look like a legitimate e-mail from someone they trust. If you and your employees don't know how to spot infected e-mails or online scams, they could compromise your entire network.

How to mitigate this risk:

- Implement employee training programs so everyone knows how to identify risks
- Simplify how employees can report a risk when they see one
- Keep your team up to date on emerging threats

2. THEY EXPLOIT DEVICE USAGE OUTSIDE OF COMPANY BUSINESS

When employees use company devices for non-work-related activities, it can create holes in your network security. It can be as simple as an employee checking unregulated, personal e-mail on a company issued laptop or smartphone while at home. If that device becomes infected, it’s a gateway to your network.

These concerns are amplified when you allow employees to use their personal devices to access the company network or data.   If that employee leaves, are you able to erase company data from their phone? If their phone is lost or stolen, can you remotely wipe the device – which would delete all of that employee’s photos, videos, texts, etc.? It can become very complicated.

How to mitigate this risk:

- Establish and enforce and Acceptable Use Policy that informs employees of how they can use company owned devices, software (including email), and internet access
- Content-filtering software and firewalls that regulate what website can be accessed using company devices or internet
- Create a mobile device management plan that includes secure BYOD options

3. THEY TAKE ADVANTAGE OF WEAK PASSWORD POLICIES

None of us need to be reminded that strong passwords are non-negotiable. Yet the most common passwords used today continues to be 123456 – reportedly used by 23.2 million different accounts according to CNN Business (April 2019). Passwords should be complex and difficult to guess and never be used in more than one place. If employees re-use passwords across platforms, access into one means access into them all.

Keep in mind that your password policy should extend to all devices, including tablets and smartphones. This can go a long way if a device is lost or stolen.

How to mitigate this risk:

- Enforce high standards for passwords and automatically prompt employees to change them frequently
- Adopt multi-factor authentication for accesses to your network and sensitive data
- Single-sign-on access limits the number of passwords employees need to use and remember

4. THEY ATTACK NETWORKS THAT ARE NOT PROPERLY PATCHED WITH THE LATEST SECURITY UPDATES

New vulnerabilities are found in the everyday software programs you use at your engineering firm – including something as common as Microsoft Office. Software vendors issue updates and patches as soon as those vulnerabilities are uncovered. It's critical you patch and update your systems as soon as they become available.

Some of the software you use works in conjunction with other software. Installing an update or patch to one can have a ripple effect and impact how two programs work together. This doesn't mean you shouldn't update it, but you should test it properly before you roll it out to your whole network.

How to mitigate this risk:

- Managed IT plans test and automate this for you, so you don't have to worry about missing an important update
- Inventory all of your devices so you know what versions of software have been installed and what needs to be updated (not all devices may have the same updates)
- Use remote access tools to roll out updates so field employees don't have to be in the office to get their necessary patches

5. THEY ATTACK NETWORKS WITH NO BACKUPS OR SIMPLE SINGLE LOCATION BACKUPS

Simply having a solid, reliable backup can foil some of the most aggressive (and new) ransomware attacks. If a hacker locks up your files and holds them ransom, your backup lets you bypass the hackers and their ransom demands.

A good backup will also protect you against an employee accidentally (or intentionally) deleting or overwriting files, natural disasters, fire, water damage, hardware failures, and a host of other data-erasing disasters.

How to mitigate this risk:

- Automate and monitor your backups so there's no doubt
- Frequently test your backups so you know you can recover your data when you need it
- Consider cloud-based solutions that back your data up to multiple locations

6. THEY EXPLOIT NETWORKS WITH EMPLOYEE INSTALLED SOFTWARE

Shadow IT is when employees install unauthorized software on company-owned devices. Sometimes they download software that to help them do their job – like a project management tool that they may have used previously and liked. Other times, they're downloading games or apps for personal use. Cybercriminals often use these innocent looking apps or games to embed malicious software. Once an employee downloads it on their phone or laptop, it has access to your network.

How to mitigate this risk:

- Shadow IT detection is available that discovers unauthorized apps and scores them for their risk potential
- Firewalls and other security solutions can prevent unauthorized downloads and you can limit download privileges on a user by user basis
- Inventory all software you install on devices so you can easily identify something that doesn't belong

7. THEY ATTACK INADEQUATE FIREWALLS

A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. Just like other points on your network, outdated firewalls can be a vulnerability. If your firewall isn't up to date or has been configured incorrectly, it can put you at risk. But all firewalls need monitoring and maintenance, just like all devices on your network. This too should be done by your IT person or company as part of their regular, routine maintenance.

How to mitigate this risk:

- Be sure the firewall you have is sufficient for your needs, is monitored, and maintained. This may require research or outside expertise
- Establish network rules specific to your users and applications
- Cloud-based firewalls make it easy to centralize how your IT team manages and maintains your firewall

8. THEY ATTACK YOUR DEVICES WHEN YOU'RE OFF THE OFFICE NETWORK

Accesses public Wifi is usually something you should avoid. Hacker can and do set up fake clones of public Wifi access points to access your device. Hackers can also "position" themselves between the public Wifi connection point and you, routing all your traffic (and information) through them. If you decide to take a risk and use public Wifi, never access any personal information that might identify you, including financial, medical or other sensitive data. It should also go without saying that public Wifi access to company or client data is off limits.

How to mitigate this risk:

- Simply don't use public Wifi and mandate that to your employees
- Use a VPN (virtual private network) which can create a secure connection to public Wifi
- Configure all your devices so they do not automatically connect to available Wifi

9. THEY USE PHISHING TO FOOL YOU INTO THINKING YOU'RE VISITING A LEGITIMATE WEB SITE

A phishing email is a bogus email carefully designed to look like a legitimate request (or attached file) from a site you trust. It used to be that there were obvious signs of a phishing email – like misspelled words or poor grammar. But they are becoming increasing sophisticated and can look very legitimate. Common approaches include a PDF for download, UPS or FedEx tracking numbers, bank notification, social media alert, or requests from common online stores like Amazon.

Careless internet browsing can also result in you falling victim to a phishing scam. Employees shouldn't be accessing unknown websites with company devices or internet access. In both cases, the hacker's goal is to get you to willingly give up your login information to a particular web site or to click and download a virus.

How to mitigate this risk:

- Your first line of defense is your employees. Train them well to identify phishing scams and questionable websites. Keep them updated on emerging threats.

- Add spam filters to your email which can detect and block many of the threats that come via email

- Secure your internet access to block access to sites which are known to be or show signs of being compromised or are illegitimate

10. THEY USE SOCIAL ENGINEERING TO EARN YOUR TRUST

Hackers who use social engineering tactics typically aren't trying to exploit software vulnerabilities. Rather, they're trying to exploit individuals to get what they need. They often use real-life interactions with employees to trick them into revealing something like their login credentials. They may pose as technical support person or co-worker on the phone, "shoulder surf" when people are using devices in public locations, or use phishing scams to get what they need.

In 2009, social engineers posed as Coca-Cola's CEO, persuading an exec to open an e-mail with software that infiltrated the network. In another scenario, hackers pretended to be a popular online blogger and got Apple to reset the author's iCloud password.

How to mitigate this risk:

- Employee education and the tactics you deploy to avoid phishing scams will also help you with social engineering scams
- Minimize vulnerabilities with usernames and passwords by adding multi-factor authentication or other identity solutions that don't use passwords.
- Hackers often start with finding information about employees on your website. Be careful about what you publish and use tools to prevent "scraping" of your website.

HOW WELL ARE YOU DOING?

Most engineering firms have different levels of security in place. But it's not always easy to stay up to speed on the newest and best tools for your business. See how you're doing with our Cyber Security Score Card for Engineering Firms at www.InhouseCIO.com/scorecard

DOES YOUR ENGINEERING FIRM NEED HELP PROTECTING YOUR BUSINESS?

At InhouseCIO, we work with small and midsized engineering firms to provide comprehensive IT services – including network security and tools that proactively protect your data. Schedule a free phone consultation and we'll help you with any question you have about IT or security.

To schedule this free phone consultation, go to www.InhouseCIO.com/consultation

InhouseCIO