Security

Protection, Lessons Learned and Employee Security Practices:

What you need to know to Secure Your Business IT

LEAPFROG®
Extraordinary IT Services

How To Build Your IT Fort: The 7 Layers of Cybersecurity Your Business Needs To Manage Now

Managing cybersecurity isn't just for other businesses anymore. You need to protect each layer of your IT kingdom before the bad guys come over the walls.

It doesn't matter that you're not as high profile as Sony or as valuable as Target. In fact, your business is MORE attractive to hackers for that very reason — your guard is probably down. And your drawbridge may even be open. Here's how to fortify your IT ecosystem to stave off breaches, thefts and even attacks from inside:

1. Equip your army.

If everyone on your team doesn't understand what's at stake and their role in cybersecurity, you can pretty much call it a day. Your IT security

team and your employees are partners! One person acting carelessly with login credentials can undermine the work and expense you put into hardening and managing your IT ecosystem. Starting now, **educate every employee** by:

- Developing clear, understandable, written policies and procedures.
- Training everyone on those procedures at least once a year.
- Keeping everyone up to date on new social engineering techniques — it's much easier to fool a person than to break through a firewall.

2. Build your moat.

Physical security in the IT world means having IT-enabled access control systems like surveillance cameras and doors that require badges to unlock. You can see (and log) who's coming and going from specific (or all) areas of your building. Access can be revoked and alarms can be triggered with a few keystrokes. You need to **create and monitor a barrier around your physical environment.**

3. Position the sentries.

Use the right devices and tools to **guard your IT perimeter:**

- Firewalls — Key IT hardware that runs 24/7/365 to block out bad traffic, let in good traffic and help you manage security by providing data on intrusion attempt patterns.
- Unified Threat Management (UTM) — Device that guards against many kinds of risks, including data leaks, intrusions, viruses, malware, web content and more. Your UTM needs to be very good and the professionals that manage it should specialize in that particular device.
- Captive portal — Tool that allows only updated, safe devices to

connect to your network. Other devices are held captive and only allowed to operate in a certain area of your network until they're secured.
- Virtual Private Network (VPN) — Provides a secure, encrypted tunnel for private communications over the public Internet. This can be critical if your company lets workers connect to your network remotely.

4. Pull up the drawbridge.

Your operating system (OS) is the doorway into your company's riches. It absolutely must be secure, stable and reliable — that's why IT pros were going nuts when companies still ran Windows XP after support had ended. Authentication processes like password management, tokens and multi-factor authentication are also critical when it comes to actions that protect **access to your platform**.

5. Hide the jewels.

Do not leave data in plain sight, whether it's at rest or in transit. **Encrypt your data!** And maybe build a private network with private encryption, if appropriate. Your cybersecurity consultant can help you decide what and when to encrypt, then monitor the encryption status of your entire IT ecosystem.

6. Barricade the tunnels.

What's the best way to find out where your applications are vulnerable? Hire a professional to break in. Penetration testing finds secret entries into your network, and vulnerability scanning tools detect new problems — application updates and new applications (especially off-the-shelf apps) can come with unintended consequences.

Harden your applications by closing each hole. And do the same with your anti-virus apps.

7. Check their papers.
Your CEO, accountants, sales reps and receptionist all have different needs to know. And so do your visitors. To prevent being attacked from the inside, segment your network into different areas and require permission to access or for transfer of data between areas — just like military checkpoints. More checkpoints, more control. Tools that **protect your internal network** include Internet Protocol Security (IPSec), port level security and Network Intrusion Detection Systems (NIDS).

When your company secures and actively manages all seven IT areas, your IT kingdom will be far, far, far safer. So the marauding armies of merciless hackers will be more likely to seek their spoils elsewhere.

What Your Business Can Learn From The Sony Hack: 3 Managed Security Lessons

The Sony hack makes one thing clear — it's time for your business to do something about cybersecurity! Yes, security can be annoying (until you need it, that is) but there's good news. **By following a harden-and-monitor approach, smaller companies can protect themselves and stop the bad guys fast. This is especially important when you don't have the resources or resiliency of a Sony-size company.**

So where do you start? With three key lessons from Sony:

Lesson #1 — Identify the hacking as it's happening, not months later.

Sony's hackers spent quite a lot of time (months and possibly a year) stealing data, as did the hackers at Target and The Home Depot. While all three victim companies had security measures in place, nothing is 100% effective and **even the best systems need to be constantly monitored to remain effective.** Managed security is the piece of the cybersecurity pie that keeps an eye on your IT environment — the goal is for security experts to spot anomalies and block intrusions before they do too much damage. It's much better to stop criminals before they've had a chance to ransack the whole place!

Note: If you don't know what happened at Sony, here's some background and a colorful timeline. Basically, hackers stole all kinds of confidential data — emails, salaries, passwords, budgets, contracts, Social Security numbers, travel visas — and made some of it public while holding the rest hostage. They also disabled computers and

demanded, among other things, that Sony not release its movie "The Interview", a comedy about the assassination of North Korean leader Kim Jong-un, or it would face mayhem at the theaters. The FBI believes North Korea is behind the hack and there's another theory from within the IT community that involves an ex-employee and pro-piracy hackers.

Lesson #2 — Use the right tools to spot intrusions.
You can't stop bad behavior if you don't know it's happening. You need tools that send up red flags. Your data, applications, internal network, IT perimeter — **all of these areas of your business need updated security tools that track, detect and report.** The bad guys keep getting more sophisticated so you have to keep up. Application control and anomaly detection engines, for example, will bubble up events where malware or social engineering techniques are being used to try to get at your company's data.

Let's say someone with administrator credentials begins uploading a whole bunch of emails that don't belong to the administrator. An anomaly detection engine will send up an alert. Then a security analyst will review the alert to see if the activity is normal or not. Not normal? Then those administrator credentials are shut down so they can investigate.

Lesson #3 — Know exactly what you've lost.
What makes not having the right tools and monitoring systems even worse? Not knowing what's missing after an intrusion! Managed security includes **forensic audit logging with an exact timeline of events.** You'll be able to identify and quantify your level

of exposure during every specific event. And you'll be able to back up your claims in court if you need to.

You'll also be prepared for extortion attempts. One of the main threats the hackers hung over Sony's head was the information that hadn't been released yet. What did they have, exactly? Was it more damaging or embarrassing? Could it irreversibly tarnish the company? Protecting your IT turf and logging unusual activity lets you keep as much of the upper hand as possible.

7 Risky Security Practices: Are Your Employees Doing Any of These?

Could your employees' bad habits be putting your company at risk? Your employees don't usually intend to be a weak link, but chances are they don't fully understand what they're supposed to do and why.

Great policies help employees develop great habits! Great policies are short, clear, specific and easy to follow. Too complicated or strict? They'll be ignored. Too vague or

loose and, well, they'll be ignored.

Do any of these people work for you? Help them out! Here's what to do:

1. Password Patty

If anyone on your team writes passwords on sticky notes or doesn't bother logging out of their computers when they walk away, your company's data can be at risk. Not everyone in your office has the same security clearance and not everyone walking around your work environment is an employee.

WHAT TO DO: Tell employees exactly how you want them to handle passwords and logon/logout.

2. Social Sam

Updating social media sites with the latest tidbit can seem harmless enough. But in the heat of the moment it's easy to overshare. A juicy comment about a project, product, client, strategy, co-worker or in-office drama may come back to bite you. Hard. And as you know, once it's out there…

WHAT TO DO: Make a clear Do's and Don'ts List for social media sharing.

3. Texting Tyrone

Who on your team has an unlimited SMS plan? Probably everyone. Texting is often overlooked when it comes to company security — by policy-writing leadership and text-happy employees alike! Sending links, images and quick thoughts by text is handy but may fall outside of what your IT department can control or access.

WHAT TO DO: Don't forget to include texting guidelines in your policy.

4. Spacey Stacey

It can be embarrassing for someone to report a lost smartphone, especially if it's happened before. Or someone can feel foolish if they suspect information was accessed on any of their devices when they weren't paying attention. If the person has a reputation for carelessness, it can be even harder to confess another mistake.

WHAT TO DO: Make it easy for employees to come clean.

5. Gullible Grace

Occasionally phishing emails make it to inboxes even if you have the latest, greatest anti-malware and firewalls. There are just too many emails bombarding the email ecosystem. So whether it's a trusting nature, curiosity or mindless clicking, some people just don't practice safe emailing.

WHAT TO DO: Clarify which emails can be opened on devices used for work (and get a good IT services partner).

6. Resentful Rudy

Sometimes it's the little things. If you're not splitting the bill with your employees for their personal smartphones when they use those phones for work (or picking up the tab entirely), you're making it easier for them to rationalize risky behavior.

WHAT TO DO: Put your money where your mouth is in your BYOD policy.

7. Efficient Evanna

Sometimes the fastest way to do something is exactly the opposite of how you want your employees to do it. Dropbox, thumb drives, emailing attachments with a gmail account — easy! Adhering to Intellectual Property (IP) policies that are too complicated or cumbersome — tedious.

WHAT TO DO: Choose systems that are safe for you and convenient for your employees.

You may also be interested in:

- BYOD Stats: What Business Leaders Need To Know Right Now
- Who Owns What? 5 Steps to Protecting Your Company's Intellectual Property
- How Phishing Emails Led To Target's Massive Breach: 5 Steps Your Company Should Take Now