Security

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

LEAPFROG®
Extraordinary IT Services

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.

LeapFROG®
Extraordinary IT Services