Security

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

LEAPFROG®
Extraordinary IT Services

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.

LeapFROG®
Extraordinary IT Services