Harvard Business Review

SECURITY & PRIVACY

See Your Company Through the Eyes of a Hacker

by Nathaniel C. Fick

MARCH 24, 2015

JP Morgan Chase. Target. Sony. Each has been part of the growing number of cyber-attacks against private companies around the world in recent years. In the latter two cases, CEOs were forced to resign in the wake of the breach. Attacks are growing more sophisticated and more damaging, targeting what companies value the most: their customer data, their intellectual property, and their reputations.

What these attacks – together with breaches to defense, law-enforcement, and military-contractor networks – reveal is that our cyber-security efforts over the last two decades have largely failed, and fixing this will require the attention not only of security officers and IT teams, but also of boards and CEOs.

Companies need to take a new approach. They can do so by looking at themselves through the eyes of their attackers. In the military this is called *turning the map around.* The point is to get inside the mind of the enemy, and to see the situation as they do, in order to anticipate and prepare for what's to come.

Unfortunately, this mindset is still too rare. Despite spending billions of dollars every year on the latest security products and hiring the best security engineers and analysts, companies are more vulnerable than they've ever been. Two trends account for this: the rapid convergence of enterprise IT architectures, and the proliferation of increasingly sophisticated adversaries.

Changes in enterprise IT over the past decade mean that every company is now a technology company. By the end of the decade, there will be 50 billion devices connected to the Internet, complicating networks and generating petabytes of data. To add to that, the cloud revolution has finally dissolved perimeters – companies enjoying the benefits of infrastructure as a service must depend upon the security of networks and systems beyond their direct control.

As mobility, the Internet of Things, and the cloud change enterprises, adversaries are also becoming more sophisticated. States and state-sponsored entities spy on and attack private companies, often using military-grade tactics and capabilities. They do this within a system where offense enjoys a structural advantage over defense because attribution is difficult, deterrence is uncertain, and attackers need to succeed only once, but defenders must succeed always.

Most companies try to deal with this chaos by parsing signal from noise. They build walled castles around their most precious assets, but perimeters don't matter when even the average college student owns seven IP-enabled devices. They rely on automated alerts to tell them when something malicious on their networks matches some previous bad event, but this approach overwhelms them with red flags while remaining blind to new and previously unknown threats.

There's just too much noise to contend with. Security analysts, for example, may see a thousand incidents in a given day, but only have the time and resources to investigate a fraction of them. This is why hackers were able to exfiltrate over 40 million credit-card numbers from Target, despite the fact that a peripheral network device had detected the malware. It's also the reason why Neiman Marcus was hacked after its system generated over 60-days' worth of malware alerts. And this is why Sony was hacked after its IT team knew the company had been under attack for two years.

By turning the map around, executive teams can learn a great deal about their own companies, and better prepare for the inevitable attacks. This is how most companies look from an attacker's perspective:

- Their security is overwhelmingly focused on generic malware detection and protection against automated threats that aren't being guided with precision.
- They don't have a full picture of what is on their networks, the cloud services they're using, the applications running on those services, and the security postures of their supply chains and partners. Their IT and security teams are peripheral concerns, costs to be managed rather than centers of excellence that support the core business.
- Overall, they are reactive, rather than proactive, in their approach to security.

Each bullet-point above is a weakness that attackers can exploit. This is why companies should learn from attackers in deciding how to defend themselves. Here's how.

1. Understand your major risks and how adversaries aim to exploit them. If security could be calculated, then adversaries would be the numerator. Companies must understand their unique threatscapes to the greatest possible extent, and generic data are insufficient. Effective security must integrate indicators of compromise (have we been attacked?), tactics, techniques and procedures (how are we being targeted?), identity intelligence (who would target us, and why?), vulnerability intelligence (what is being exploited in the wild?), and attack attribution (is this commodity or targeted?). Only with focused threat intelligence can analysts spend their precious and valuable time investigating the most important incidents, prioritizing those associated with your most formidable adversaries and your greatest business risks. You can go crazy (and broke) trying to play Whack-A-Mole in defense against them all. Instead, identify your most essential assets and focus scarce resources only on those threats that actually pose a risk to your company.

2. Take inventory of your assets and monitor them continuously. If security could be calculated, then inventory would be the denominator. At the simplest level, companies must identify and monitor all of their interconnected assets: is a developer spinning up a thousand virtual machines without your knowledge? What applications are running on the database servers holding your most valuable information? Did an employee connect a new device to your corporate network? Does one of your distant subsidiaries have a new partner? Does your HVAC system connect somehow with your Point of Sale? Periodic assessments, reports that take weeks to prepare, and conclusions that require complex interpretation contribute to gaps in security. Companies must maintain a dynamic, real-time inventory of assets, monitor those assets continuously, and render them visually in way that is simple and intuitive for security and operations teams.

3. Make security a part of your mission. The prevailing approach to security is compliance-focused, cost-constrained, peripheral to the core business, and delegatable by C-suite leaders. Working on a team like that isn't fun inside any enterprise, and it loses against 21st-century adversaries who know that it's more fun to be a pirate than to join the Navy. Any defense is only as good as the people doing the defending. The new model of security needs to be about mission and leadership, ensuring that we have the best defenders up against the best attackers. Security is no longer delegable, and the mission of security teams must be synonymous with the mission of the company.

4. Be active, not passive, in hunting adversaries on your network and removing them. The term "active defense" has been tarred as a euphemism for "hacking back," and companies are ill-advised to go on the offensive: first, it's illegal to access others' networks without permission, even if you're acting in supposed self-defense; and second, it's just not smart to escalate unless you can dominate, and even the biggest companies will ultimately lose against state or state-sponsored adversaries. So while you cannot go attack the other team on their own turf, you can and increasingly must be active against adversaries inside your own networks. This means assuming not merely that you are under attack, but that your attacker is in, and so you must hunt for a stealthy, persistent human adversary in order to contain and remediate the risk *before* they can cause damage – dramatically cutting the time between breach and detection from its current average of more than 200 days.

It is easy during these days of frequent and devastating attacks to cry out that the sky is falling, and that the very future of the Internet as a trusted domain of commerce and communication is at stake. But it would be wrong to extrapolate the data points of recent years into a line leading to ruin. Too many of us have too much at stake here, and the combined forces of executives, entrepreneurs, software developers, security teams, and investors all turning the map around can equip us to defend against this next generation of adversaries.

Nathaniel C. "Nate" Fick is a former United States Marine Corps officer and the CEO of Endgame. He is the author of *One Bullet Away: The Making of a Marine Officer*.