DON’T BE A “HACKER SNACK”: CYBERSECURITY DONE RIGHT

True cybersecurity isn’t about preventing every threat; it’s about properly handling the inevitable

Cyber thieves have a name for a firm that mistakes prevention for comprehensive threat planning—a “hacker snack.” Hard on the outside, soft and gooey on the inside.

Unfortunately, too many firms are satisfying those illicit cravings.

The problem, says Daimon Geopfert, national leader of security and privacy consulting at RSM US, is that many firms started from the perspective that if their systems got breached, they did something wrong. The reality, Geopfert says, is that no firm can prevent all attacks.

“This is a basic 80/20 problem. You can address 80 percent of your issues with 20 percent of your effort. Fixing that last 20 percent requires significant effort and expense and will never reach zero,” Geopfert says.

Well-managed firms spend lots of effort to detect and correct breaches once the inevitable happens. That requires a holistic approach that goes well beyond efforts to protect every point of entry. Not only will it eventually fail; it often costs more than necessary, Geopfert says.

Ultimately, the prevent-at-all-costs approach starts with the wrong question: How do I keep everyone out? Instead, Geopfert says, firms should first ask: What am I trying to protect?

CODE RED

“We had one engagement recently where the client was running Windows ME.”

↓ CONTINUES ON NEXT PAGE

Know Your Data

The holistic cybersecurity approach is based on three core efforts: Protect, Detect, Correct.

Protection goes beyond the traditional concepts familiar to anyone with a laptop—firewalls, anti-virus, and keeping software up to date. Instead, it first requires understanding the types of data your firm handles and figuring out what requires the greatest level of protection.

"You want to think in terms of 'layers of trust,'" Geopfert says. He says the best example comes from the physical world—an office building. When you enter a building, there's typically some form of security in the lobby, and then additional security protocols in place for sensitive areas like a data room.

Yet that isn't how it often gets structured in the virtual world of data.

"It's like once you get past the security desk, everything is in the lobby," Geopfert says.

The layering approach acknowledges that some data is more sensitive than others and therefore should be sectioned off from less critical information. And only those who need access should have it, and only the systems that need it can actually reach it.

WARNING AHEAD

"I asked one client where their IT infrastructure was. They laughed."

Know What's Normal

Once you've prioritized and protected your data, you need to plan for the inevitable breach. Doing that requires pairing internal knowledge with software to define the normal and abnormal. Without that, there's no way to identify suspicious behavior. Geopfert says that a Verizon study found that 87 percent of firms that experienced a breach had access to the information needed to detect it, but were incapable of identifying it.

Luckily, he says, much of the most critical data is often relatively static, so it's easiest to get a handle on it. Segmenting the critical data and systems away from day-to-day user systems and data, which is typically "noisy" but less critical, helps bring the real issues into clearer focus.

"There are some very binary use cases—if thing 'X' happens, it's bad," Geopfert says. "To get to the point where you can detect nuanced issues, such as changes in user behavior, there's much more you have to do."

Doing more involves using a combination of behavioral, trend, and heuristic information to define and trigger warnings. For instance, Geopfert says, picture a user who has never logged in before 7 a.m., never later than 7:30 p.m., has only touched five systems in the network, and only from three geographic locations. If that user logs in at 2:30 a.m. from a fourth location and proceeds to access other systems, then that should trigger an alarm. But a system can only be set up to "listen" for such events through careful study of existing patterns.

Know What to Do When Disaster Strikes

How a firm reacts when a breach occurs is as important as the steps meant to prevent and detect it. In fact, in combination with the layering approach detailed above, incident response is a key target of regulators, state attorneys general, and insurers—in other words, the groups that can make life after a breach particularly miserable.

The simplest advice, Geopfert says, is don't go it alone. Internal teams should not be tasked with cleaning up an attack once it occurs. They should be technically capable of identifying a breach and then putting a response in motion—calling law enforcement, shutting down systems, alerting the public—but shouldn't do the forensic work.

"Unless they're a *Fortune 50* company, they probably don't have the budget to have that staff in-house," he says. "Most organizations that try to do this themselves throw up their hands after a couple of weeks and call in an outside firm. There have been cases when insurers won't pay fines because the firm didn't properly handle the fallout, and while they were attempting to do the right thing, they actually extended the duration and damage of the event."

The best firms will put together a great plan, often with a consultant, and then run through it a few times a year. A practical approach works best.

"Don't overthink it," Geopfert says. "One of my clients has everyone on the team bring in news articles of breaches. They throw them on the table, go through them and discuss how they would respond. It's extremely effective."