solarseven/Getty Images

To survive in the age of advanced cyberthreats, use 'active defense'

Brad Brown, Daniel Ennis, James Kaplan, and Jim Rosenthal

Anticipating attacks, responding to them in real time, setting traps to contain them, and protecting assets according to their value can help companies stop sophisticated cybercriminals.

For all the resources devoted to improving cybersecurity, threat levels continue to rise faster than defense capabilities. The WannaCry ransomware attack in May 2017 offers a case in point. Hackers helped themselves to tools stolen from intelligence agencies and others and created havoc around the world, forcing systems off-line at the Chernobyl nuclear power station, affecting several parts of Britain's National Health Service, and interrupting scores of computer systems. The relatively unsophisticated nature of the attack limited the overall take. Yet, it reveals just how vulnerable organizations are to even rudimentary hacks done at scale. Imagine if the attackers actually had their acts together.

Some do. Several of the world's best-protected organizations have been attacked over the past few years, including a number of preeminent government agencies and technology companies. Hackers who may once have been groping around in the dark are acquiring a deeper understanding of who they're targeting and how to get inside. Thanks to a proliferation of botnets[1] and the easy sharing of tools on the dark web, the expense of mounting cyberattacks is also plunging. Put it all together, and criminals, some of whom are state sponsored, have ready access to cash, technologies, and resources. Over the coming years, crimes in the cyberrealm are predicted to cost the global economy $445 billion annually.[2]

Perversely, the high-profile hacks may have done us a favor. For a long time, cybersecurity experts have proselytized about the evolving threat landscape. But like doctors who caution their patients to avoid sedentary lifestyles, the risks these experts describe seem important but distant. The WannaCry attack—its brazenness, the speed at which it scaled, and how effortlessly it derailed business as usual—took cyberthreat activity from a slow-moving abstraction and made it real.

Businesses must consider themselves warned. Rather than continue in a passive stance, organizations must adopt an "active defense" model: they should assume their firewalls will be penetrated. They should assume that encryption keys will be compromised, and that hackers will stay a step ahead of them in deploying malware in their infrastructure. Active defense requires organizations to anticipate attacks before they happen, detect and respond in real time, establish traps and alarms to contain attacks, and adopt a tiered approach to protecting critical assets.[3]

Understanding the challenges

The threat environment is constantly changing, but how businesses have responded to those threats has remained largely the same. That's not going to work anymore. Here's why:

- **A significant number of breaches are still caused by employee lapses:** Despite years of training employees on good data data-hygiene practices and continued investment in malware and virus detection, the majority of corporate data breaches are caused by simple human error: clicking on an innocent-seeming email, downloading a legitimate-looking attachment, or revealing identifying information to a seemingly trustworthy source.[4] Even if two-thirds of employees avoid these traps, about one-third will still fall prey (and about 15 percent of this group will go on to become repeat victims).[5] That means an automated barrage like a phishing campaign that blasts messages to thousands of employees is assured a reliable percentage of hits—and this is just by using basic techniques. More devious attackers can do extensive damage. All it takes is one or two employees to expose their credentials, and an attacker can decrypt them and make their way inside. Most organizations are not set up to thwart this behavior.

[1] A network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

[2] *The global risks report 2016*, World Economic Forum, 2016, weforum.org.

[3] In this article, we define "active defense" as all actions aimed at anticipating, detecting, diverting, and isolating cyberattacks. We specifically exclude potentially illegal actions, such as hacking back.

[4] *2017 data breach investigations report*, Verizon, 2017, verizonenterprise.com.

[5] *Data breach digest: Perspective is reality*, Verizon, 2017, verizonenterprise.com.

- **Perimeter and encryption defenses aren’t enough:** Large organizations have spent millions on firewalls and encryption. But the strongest perimeter defenses won’t keep a company safe if intruders are already inside—and given the earlier point regarding internal threats, businesses must assume some are. Once there, intruders can stay for months, acquiring information and using that information to enter the systems of other companies. Criminals know that the best targets are well defended, so rather than trying to penetrate a heavily secured front door, they can go around to the back, to the company’s supply chain. Data show that 63 percent of data breaches come from exploiting weak points in a company’s customer and vendor network.[6] One major consumer-goods chain, for instance, suffered a major loss when attackers climbed in through the proverbial ducts—by hacking the company’s air-conditioning vendor and working their way in. Companies need to do more than bar the gates; they need to monitor their entire network (and, in some cases, their network’s network) to anticipate where attacks will come from. But most organizations don’t have that capability.

- **IT organizations are overwhelmed and under-resourced:** Challenging the IT and security organization to keep up with the latest attacker moves is unfeasible. After all, hackers may only need a blunt tool and a few resources to exact a toll on one target. IT organizations meanwhile have to stay alert to thousands of external threats from a variety of sources. They need to be able to filter out the most pertinent intelligence, and have a sufficiently detailed understanding of where their most critical data assets are stored, and as well as what could put those assets at risk to secure them properly—all the while continuing to support the IT needs of the entire business. Trying to manage all these demands can lead to indecision and conflicting priorities. An effective response requires expertise and capabilities to detect, deter, and defend against these risks. But while some companies, such as large banks and telecommunications organizations, have been able to build credible defenses at that scale, the spending level required can stretch to the hundreds of millions. Few organizations can match that.

We are likely to have more malicious actors entering the field, more attacks that take advantage of basic loopholes, and more players capable of launching sustained, pernicious insider-based attacks. New strategies and partnerships are required.

Shifting to an active-defense model

Active defense allows organizations to engage and deflect attackers in real time by combining threat intelligence and analytics resources within the IT function. The approach draws upon lessons the military community learned in defending itself in fluid attack environments like Afghanistan and Iraq. To ferret out and respond to risks faster, commanders began positioning operators, planners, and intelligence analysts in the same tent where they could feed special operations teams with ongoing, real-time information. Integrated and more accurate intelligence made it easier for units to track chatter, identify targets, and increase the

[6] *2016 data breach investigations report*, Verizon, 2016, verizonenterprise.com.

number of missions they could conduct over the course of an evening.

In recent years, some large organizations have applied that thinking to bolster their own defenses. A major financial-services institution, for instance, greatly enhanced its cybersecurity capabilities by convening a team dedicated to providing active defense. The team established state-of-the-art threat-monitoring capabilities so it could continually scan the company's ecosystem—its own network as well as the broader supply chain—for unusual patterns and activity, sniff out potential threats, and thwart attacks, often within minutes of detection. It has impeded thousands of attacks as a result.

Few organizations have the budget to build dedicated centers of this scale. But there are other ways to access needed capabilities. By realigning the existing budget, engaging outside resources, and forging information-sharing partnerships, businesses can still mount a strong active defense. Success in doing so starts with understanding what's involved. Here are the central elements of an active-defense posture:

- **Anticipate attacks before they happen.** If the old model was all about defending the organization with layers of perimeter protection, the new model is far more proactive. Businesses need to scour the threat environment to find out if someone is talking about them or someone in their chain, pinpoint software and network vulnerabilities, and spot potential hacks before they occur. This is an intelligence-heavy, data-driven process—and it's critical. Bringing cybersecurity experts into the tent can help organizations gain the insights needed. Third parties that specialize in threat intelligence monitor a wide range of sources. That includes following threads and conversations in places like the dark web—websites that require special software to access and provide user anonymity—to gauge evolving threats to the company or its vendors.

- **Detect and respond to attacks in real time.** Early detection depends on an organization's ability to track network patterns and user behavior that deviate from the norm. The challenge is to figure out what normal is, given that businesses are constantly changing and human behavior is unpredictable. Intrusion detection and anomaly detection are two widely used approaches. Intrusion-detection systems (IDS) look for misuse based on known attack patterns. However, because these systems are trained to spot defined-threat signatures, they may miss emerging ones. They may also have a hard time distinguishing problematic activity from legitimate activity, such as innocuous internal communications that contain flagged language or Internet addresses (for example, malware warnings), ongoing network-security-vulnerability scans, or attacks against systems that have already been patched. Anomaly-detection models work the other way around. Instead of looking for known attack signatures, they look for behavior that deviates from typical network patterns, such as an unusual spike in volume. Companies with an active-defense posture use both IDS and anomaly-defense systems to provide more comprehensive threat detection.

- **Establish traps and alarms to contain attacks.** Decoy servers and systems, known as deceptions, are another tool that companies can deploy as part of their active defense. Deceptions lure attackers into a dummy environment where they can be studied to gain additional intelligence. Entrance into the trap sets off an alarm, alerting the threat-operations center and triggering software agents and other deterrents to be placed in the network to close off access and prevent damage to the business. Some businesses also salt these environments with false information to confuse attackers. Once intruders breach a system, they usually return through the same gateway. Deceptions and other traps need to be convincing enough facsimiles to keep intruders inside long enough for the company to gather useful insights. Companies can then use those repeat visits to record the methods attackers are using to gain file, system, or server access and update their defenses accordingly.

- **Use ring architectures to protect critical assets.** Over the longer term, businesses need to construct layers of defense to keep the company's most critical assets deeply buried. Ring architectures, for instance, allow organizations to store data in different layers depending on the value and sensitivity of those assets. Each layer requires a specific key and authorization protocol to manage access. Penetration in any one layer will set off alarms. Active defense also requires an IT plan that organizes and prioritizes security-related technology spending. Otherwise, it can be tempting to try to protect everything and in the end create vulnerabilities when spending and systems prove too difficult to maintain.

Taken together, these measures can make a profound difference. At one financial institution, for instance, intelligence gathered on the dark web revealed that an overseas criminal syndicate was seeking to access the credentials of the bank's high-net-worth clients. Analysts informed their IT counterparts, all of whom worked together in an integrated active-defense unit. Engineers spotted command-and-control-type traffic emanating from PCs associated with high-income zip codes and found a pattern of anomalous log-ins for some of their high-net-worth accounts. The threat center immediately activated a forced password reset for affected customer accounts and placed temporary holds on all wire transfers in excess of $100,000. In addition, it reimaged affected desktops and issued a communication to select high-net-worth customers, encouraging them to implement two-factor authentication. This quick, coordinated response prevented sensitive information from being compromised.

Getting started

Knowing the core elements of an active-defense model can help organizations realign their cybersecurity spending, integrate analytics with intelligence-gathering processes, and provide tighter ongoing coordination. By pinpointing the critical holes in their defense structures, businesses can then determine where it makes sense to acquire needed skills, tools, and expertise and where they can partner with others to fill those voids.

As with any new approach, making the case for change is critical. Shifting to an active-defense posture requires leaders to recognize that cybersecurity requires top-level oversight and commitment, backed with the right budget, authority, and performance incentives to make it real. Organizations looking to implement an active-defense model must also recognize that changes in traditional working practices are required. Some of those changes may be uncomfortable. Given the sophisticated nature of some attacks and the prospect of state-sponsored intervention, companies accustomed to keeping intrusion activity closely guarded may need to open up and work more collaboratively with peers within and across their industries to share notes, best practices, and resources. Such collaboration can take place within industry associations like the Financial Services Information Sharing and Analysis Center, which shares threat intelligence and incident information across nearly 7,000 financial-services institutions.

Changes across the broader security ecosystem are also necessary. The best partnerships will bring together a mix of government, technology, and business leaders to create an open and ongoing exchange of information. The vendor community also must adapt. They need to evolve their offerings from chasing down alerts to providing a range of sophisticated services similar to those that major banks and telecommunications companies have built for themselves.

Collectively, better intelligence, smarter analytics, and stronger collaboration can help organizations build the active-defense capabilities they need to respond more effectively to pervasive, advanced cyberthreats. ◆

Brad Brown is a director emeritus in McKinsey's Boston office and an ongoing adviser to BlueVoyant, **Daniel Ennis** is the head of threat intelligence and operations at BlueVoyant and the former director of the National Security Agency's Threat Operations Center, **James Kaplan** is a partner in McKinsey's New York office, and **Jim Rosenthal** is the cofounder and chief executive officer of BlueVoyant.

Digital/McKinsey

November 2017
Designed by Global Editorial Services

McKinsey.com
@DigitalMcKinsey
facebook.com/DigitalMcKinsey