You're breached! Balancing the threat with considered defenses

You've made your plan for defending against an active attack. Now the attack is happening. Are all your ducks in a row? *Are you sure?* Evan Schuman looks at what CISOs do right and wrong.

One of the most frightening situations in enterprise security operations is when security analysts begin fighting what appears to be an active attack, fully cognizant of the horrors that could happen if the attack is not neutralized immediately — or if their defensive plans are wrong. But the security analyst in charge when the attack is first detected, perhaps at 3 a.m., also knows that shutting out an attacker too soon could be equally terrible and that the initial information the analyst has in hand will invariably be proven wrong by later forensic analysis.

Indeed, the typical attacker will do everything possible to hide details and will likely leave bogus details in the security log to mislead analysts deliberately about what is going on. Generally speaking, the initial analysis of a large percentage of attacks is simply incorrect.

Is the attacker a 14-year-old would-be cyberthief looking to make a name for themselves who will flee at the first sign of resistance or is it a state actor backed by seemingly infinite funding and resources from a rogue nation? Frustratingly, a state actor might initially look like a teenager and that teenager might deliberately mimic actions performed by state actors.

In the 12 minutes or so that an analyst must make critical decisions, the lack of trustworthy information makes almost any decision highly risky. And making no decision is the riskiest choice of all.

Not-so-rapid response

One of the top mistakes with security knights trying to slay cyberdragons is that they "overestimate the sophistication of an attacker," says Curtis Fechner, a principal consultant of threat management at systems integrator Optiv. "During an active attack, I've seen leaders greatly overestimate the capabilities of those attacking them. Attacks of opportunity are very common. There's often an immediate knee-jerk reaction to do rapid containment. What does that do for the business?"

Fechner says that there is too little thinking through the likely impact of the decision. "What are you accomplishing by jumping up with your hair on fire?" he asks rhetorically, noting for sophisticated attackers, "if you tip them off too early, you're revealing all of the cards in your hand."

Robinson Delaugerre, head of incident response at Orange Cyberdefense (OCD), the cybersecurity group within French telecommunications provider Orange, agrees that during the initial minutes after identifying an ongoing breach, the analyst probably does not fully understand the scope

OUR EXPERTS: Active risk management

Todd Carroll, CISO, CybelAngel; former FBI cyber expert
Robinson Delaugerre, head of incident response, Orange Cyberdefense
Curtis Fechner, principal consultant of threat management, Optiv
Yehuda Lindell, professor of cryptography, Bar-Ilan University
Mario Paez, director of cyber, Marsh & McLennan
Brian Reed, senior research director, Gartner
Curtis Simpson, CISO, Armis; former CISO, Sysco

55%

Percentage of U.K. companies that reported cyberattacks in 2019

– Hiscox Cyber Readiness Report 2019

and type of attack. "In the first six to ten minutes, even in the first hour, you probably have no idea what you're witnessing. The qualification is usually done wrong and [analysts] act far too quickly," he says.

A common issue is that what appears to be a new, active attack actually is an attack that could have started months earlier, but the attacker just made a mistake that triggered security's attention.

Curtis Simpson, CISO, Armis

The quick action can be problematic. "Their first instinct is to block this traffic and to clean the machine to reformat and to rebuild it. If this remediation action doesn't succeed, you have no way of knowing it," Delaugerre says. "You have blocked what you know is bad, but you have lost the opportunity" to learn as much as possible.

"You don't know if the malware has been dropped by something else," he continues. "You lose your strategic advantage over the attacker. What if you had not identified properly the attacker's command and control?" That will force the attacker to go even more stealth. What you want to learn, though, is how the attacker exploited your network.

> "If you tip them off too early, you're revealing all of the cards in your hand."
>
> *– Curtis Fechner, principal consultant of threat management, Optiv*

Delaugerre elaborates: "The common mistake that [the security teams make] is that they think they have enough information to act meaningfully in the early minutes when detecting an incident. When they receive a report of an incident, it's easy to assume that either the incident would be automatically remediated — possibly by their existing antivirus — or alternatively, [the team can] then decide on an action that is based only on a partial understanding of the incident detected."

That, he continues, "was the case with a manufacturing client of OCD. When they detected malware on a couple of their servers, their initial reaction was to block all IP addresses they had detected as command and control servers from analyzing the sample. Such a response would actually have removed all of the agents from our client, since they would have blocked all indicators they could detect, but not given themselves more information about the threat agent, their objectives, the extent of the foothold they had.

"It would also have alerted the threat agents that their presence had been detected," he continues. "Our incident response team proposed additional measures — to check proxy logs and other sources to identify other suspicious behaviors from compromised machines and perform a deep, forensic analysis of a sample of compromised systems to identify if other means of command and control were in place. With the additional time and measures taken, we were able to gather more specific information about the source and purpose of the cyberattack, and ultimately fully contain the attack."

Delaugerre's point is important, but especially when examined with hindsight. But as a practical matter, it might not always be viable. Analysts need to make split-second decisions and waiting for a deep, forensic

17%

Global location analytics market expect to grow by 16.6% to $29 billion by 2024

– MarketsandMarkets

analysis could take a considerable amount of time. It is a hard call to make.

Keys to the kingdom

In any security team, the questions that must be addressed speaks to responsibility — who does what and who has access to the highest priority data? Ultimately, one seemingly counterintuitive but crucial answer keeps coming up for this question: During the course of a data breach response, who should have ultimate access to all corporate data? Although security analysts argue that they need *all* data immediately, CISOs and others are much more cautious: No one.

Even though it is certainly essential for security teams to have the tools, time and resources they need to identify and stop a breach, no single individual, whether the CISO, CIO or any other C-level executive, should have total access to all data assets, some have argued. This is not unlike the requirement in the military to have two keys held by different officers needed to launch a nuclear weapon — separating responsibility is one additional level of security.

One issue is whether CISOs and CSOs, as well as other C-level executives and line-of-business department heads, will give those security analysts enough tools and resources to make those decisions. Who is in charge and who has access to which assets should be sorted out early in the incident response policies and procedures.

It is understandable that the executives heading the team will expect to have direct access to everything they might need to fight the attacker successfully, as well as any files on the network. However, allowing a single employee to have full privileges and access to everything, from internal systems to those controlled by key partners, is a security nightmare waiting to happen.

Curtis Simpson is no stranger to big-company security challenges. While currently CISO for Armis, an IoT security company, Simpson previously spent more than 11 years in cybersecurity management at the multinational corporation Sysco, a marketer and distributer of food products to restaurants, hotels, healthcare and educational facilities that currently is ranked 54 on the Fortune 500. He served his final 18 months at Sysco as vice president and global CISO, leaving the company in early 2019.

> "In the first six to ten minutes, even in the first hour, you probably have no idea what you're witnessing."
>
> *– Robinson Delaugerre, head of incident response, Orange Cyberdefense*

Simpson argues that granting full access would indeed potentially cause new security problems. "No one can have carte blanche credentials to everything. In eight out of 10 of these scenarios, the analysts are blowing a scenario out of proportion," Simpson says.

For security analysts, the access issue is "a balance of [the] inconvenience versus being frustrated," Simpson says. In his operation, analysts could check out temporary access to much of what they needed, though that could cause a frustrating delay during an active fight.

But Simpson also points out that it is more typically a corporate political issue, which the CISO alone cannot necessarily fix. "More commonly, there's some area, like infrastructure, that doesn't want to share access," he says. That department head "has really dug their foot into the ground, saying 'You can't have this.'"

Yehuda Lindell, a professor of cryptography at Bar-Ilan University in Tel Aviv, argues that a decision to take down part of the network, disconnect the company from the internet or even shut down selected servers is scary for analysts because it requires up-to-date understanding of anything and anyone who needs those

93%

Percentage of cyber incidents can be prevented with basic cyber hygiene

– 2018 Cyber Incident and Breach Trends Report, Online Trust Alliance

resources to function, whether it is an employee, partner or customer.

"Let's first define what critical operations means, without completely bringing everything to a screeching halt," Lindell says, noting that attackers often generate false positives deliberately "to make analysts hesitant to shut anything down."

Yehuda Lindell, professor of cryptography, Bar-Ilan University

A psychological factor complicating the shutdown decision is geographic bias. An example would be an analyst working from headquarters at 3 a.m. Eastern Time in the U.S., who might think that a brief shutdown would not be that disruptive, even if it is a global company with customers and employees around the world. "Geographic bias makes 100 percent sense," Lindell says.

That bias, however, could have a serious impact on a company. A 3 a.m. shutdown in New York, for example, might not mean much since most employees are home asleep, but customers in Munich are just starting their day at 9 a.m., while in New Delhi it would be 1:30 p.m. Geographic bias ultimately could have a serious impact on a shutdown decision, particularly if the shutdown eventually turns out to be overkill.

> "But too often CISOs that report to CIOs are stifled."
>
> *– Todd Carroll, CISO, CybelAngel*

Lindell argues that analysts sometimes do not think through the impact on cryptographic controls during an active attack.

"Most people don't think about their cryptographic infrastructure in the context of threat response. However, this is a huge mistake. In the case of a breach, are you able to quickly shut down cryptographic services that can be used maliciously by an attacker in the network? Even if your keys are protected in the best possible HSM (hardware security module) or other key protection mechanism, an attacker who breaches the machine that is authorized to use the keys can cause significant damage," Lindell says.

"If you have no way to shut this down, you may not be able to stop this damage," he continues. "Needless to say, this is not trivial since we want to be able to shut down some functionality, without preventing critical processes from continuing. This challenge is exactly why this scenario has to be planned for in advance."

Even after the breach has been successfully mitigated, Lindell says, security teams must pay attention to crypto services.

"The fact is that many cryptographic keys are not well protected and are vulnerable to theft by attackers who have breached a network. Companies should have processes in place to enable fast and automatic key rotation so that this risk can be mitigated after an attack has been discovered. If this needs to be done manually, or many different key managers over many sites are needed, then this will be a painfully long process that leaves the company vulnerable," Lindell says. "In some cases, the process can be so painful that organizations don't rotate keys unless there is explicit evidence that they were compromised. A good strategy built ahead of time for how to deal with this can enable a fast response, reduce vulnerabilities and save considerable time."

Corporate culture

Todd Carroll spent more than 20 years in various senior cybersecurity roles with the

33%

Percentage of companies that say they have been impacted negatively by the cybersecurity skills shortage

– ESG

FBI, including assistant special agent in charge cyber and counterintelligence branch, now works as CISO for French security consultancy CybelAngel. He says that he typically places the blame for a security analyst's can't-win, active-threat dilemma with senior management.

Todd Carroll, CISO, CybelAngel

Security policy needs to be flexible enough to allow the analyst to react to what surprises the attackers offer, he says. It should provide guidelines for when different systems should be shut down, but it must allow for unanticipated attack methods. Sometimes, CISOs and CSOs will try and be highly specific in policies for analysts, so that it is explicit about what justifies a shutdown and when and what does not.

But Carroll has seen some CISOs getting too prescriptive, which makes it harder for analysts dealing with unexpected attack methods. "If you're writing at that level," he says, "you're done."

He continues, "The problems start with the organizational structure. At the [FBI], that was one of the first things we'd want to assess when working with large enterprises — how are information security responsibilities allocated across the C-suite? I don't think the CISO community has quite solved this yet. I'm of the opinion that the CISO should not report to the CIO," he notes.

"That may work in some organizations, especially those with a very progressive CIO," Carroll continues, "but too often CISOs that report to CIOs are stifled. I think CIOs are evaluating and implementing new technologies without letting subordinate CISOs properly advise on the risk those technologies pose. If the rest of the C-suite views the CIO as a value creator, and a subordinate CISO as a 'but wait' or 'what if?' role, then the CISO's perspective is at risk of being discounted," he says.

Some CIOs inadvertently muffle the voice of the CISO that should be assessing new technologies from a security point of view, he adds. In some cases, a conflict develops between the two roles.

"Many CISOs are forced to play politics and acquiesce to the CIO's technology initiatives," he says. "These CISOs can become content to simply plan for controls and patches to accommodate new technologies driven by the CIO.

"When reporting to the CIO, CISOs are often envisioned by the rest of the C-suite as having a 'Break Glass in Case of Emergency' label affixed to them," he continues. "And I wish the rest of the C-suite would appreciate the business value of the CISO's charge. It has the same impact on the bottom line that the C-suite expects to be evidenced by the CIO. This isn't obvious to every organization."

Carroll argues budgets and vendor selections need to happen more informally. "I think enterprises evaluate budgets and vendors too formalistically when they should be more responsive. And I don't think enterprises are tailoring their information security spend to the idiosyncrasies of their organization, industry, business model, etc. Not enough CISOs and CIOs think about this.

"[CISOs] should be asking themselves: What data is really important or most valuable to us? What kind of breach or incident would really debilitate the organization? What are our unique cybersecurity weaknesses? They should design their information security stack around those answers. Information security is not about checking boxes. Go bespoke, not off-the-rack," Carroll says.

52%

Percentage of IT pros who say security is among their biggest networking challenges for supporting container-based applications

– ESG

Missing seat at the table

Another key corporate issue is who is at the table when active threat policies are crafted. The usual suspects generally include security, IT, legal, network operations, communications and perhaps some other senior-level executives. Mario Paez, director of cyber for the Marsh & McLennan insurance agency, makes a compelling argument for adding the CFO and a senior representative of the cyber insurance provider. Although the argument sounds decidedly self-serving for an insurance company, his explanation makes a lot of sense.

Mario Paez, director of cyber, Marsh & McLennan

One of the top executive-level concerns, especially with the CFO and the board of directors, is to understand who will pay for the costs of fighting a cyberattack. This becomes even more problematic when some costs are seemingly self-inflicted, such as having to shut down servers or network access in areas where it will sharply impact revenue.

> "Look at security incidents as a technology problem rather than a business problem, which is what it really is."
>
> *– Brian Reed, senior research director, Gartner*

When crafting policy guidelines, a CFO wants the insurance exec right there, agreeing or disagreeing with phrasing and what the guidelines will say. Specifically, the idea is to have the insurance sales representative sign off — in writing — on the amended policy wording, guaranteeing that, as long as the analysts follow the policy as closely as practical, the insurance company will cover the resultant financial damages.

"What if [the enterprise analyst] decides to shut [the network] down at minute five and your insurance doesn't provide for that?" Paez asks. Is that really something that the CISO and CFO want to discover after the fact? Having the insurance representative meeting with the senior executives to discuss financial issues and protections also has the added benefit of giving far more credibility into the demand that these policies must be observed.

Having your insurance company sitting at the table with corporate decision-makers might seem counterintuitive, however, any first-year law student will tell you that the proverbial devil is in the details, and what constitutes meeting your obligation to file an insurance claim is one very large detail. According to Paez, this simple step can prevent a lot of questions and concerns later, eliminating surprises and possibly a very large and unanticipated financial hit.

Gartner Senior Research Director Brian Reed says that this helps align all security into internalizing the financial implications of these security decisions. Analysts "look at security incidents as a technology problem rather than a business problem, which is what it really is," Reed said. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@cyberriskalliance.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at (347) 480-1749, or via email at david.steifman@cyberriskalliance.com.

88%

Percentage of small businesses that say they know they will be targets of cyber attacks

– National Cyber Security Alliance