by MIT Technology Review Custom, in partnership with Hewlett Packard Enterprise Security Services and FireEye Inc.

Crisis Communication After an Attack

If there's one area where organizations stumble when responding to breaches, it's in keeping stakeholders informed. Doing that job well starts well before cybercriminals come calling.

Here's an increasingly common scenario: You're a business or IT leader, and you learn—quite possibly from sources outside your company—that cyberattackers have compromised your organization's systems. You don't know yet how serious a breach you're facing, but it's clearly time to activate your crisis-communication plan.

Except that you don't have a plan. Or you have one, but it doesn't cover cybersecurity crises.

In either case, you're not alone. Security experts say even the most security-conscious organizations are often woefully ill-prepared when it comes to communicating with internal and external stakeholders during and after cyberattacks—and that leaves them scrambling to regain control in a crisis. That's typically because they didn't do enough work before the breach.

"The biggest mistake I see companies make is not having a crisis-communication plan in place," says Vitor De Souza, vice president of global communications for FireEye Inc., a leading global cybersecurity firm. De Souza's observation is supported by a February 2016 survey conducted by MIT Technology Review Custom in partnership with FireEye and Hewlett Packard Enterprise (HPE) Security Services. Forty-four percent of the 225 business and IT leaders polled said their organizations didn't have cybersecurity crisis-communication plans in place; another 15 percent didn't know whether they had such plans.

A similar mistake: relying on a crisis-communication plan that focuses on other types of emergencies—fires, power failures, natural disasters. This kind of plan won't address how to communicate about issues unique to information-security breaches, such as possible cybercriminal access to personally identifiable information or corporate intellectual property.

Cyberattacks are more complicated to deal with than fires, and they are far more complicated to discuss with the public. "If there's a fire in the building, there are one or two ways out, but in cyberspace, there are many different scenarios. You have to know what you might be facing," De Souza says.

"As individuals in an organization, if we smell smoke or see a fire, we feel empowered to sound the alarm," says Andrzej Kawalec, CTO of HPE Security Services. A fire alarm activates emergency-response and crisis-communication plans in a fairly straightforward manner, but, Kawalec says, this doesn't happen with cybersecurity incidents, for two reasons.

44%

Percentage of business/IT leaders whose organizations lacked cybersecurity crisis-communication plans

15%

Percentage of business/IT leaders unsure whether their organizations had cybersecurity crisis-communication plans

Source: *Cybersecurity Challenges, Risks, Trends and Impacts Survey,* MIT Technology Review Custom in partnership with Hewlett Packard Enterprise Security Services and FireEye Inc., 2016

First, breaches are often first reported by outsiders, catching organizations by surprise. In 2015, 53 percent of the incidents handled by Mandiant, a FireEye company, were first brought to companies' attention by external sources, such as customers, partners, law-enforcement officials, journalists, or the attackers themselves. "Immediately, they are in a very reactive situation, with a large degree of uncertainty," Kawalec notes.

> "A breach is not an IT problem. It's a business problem. The C-suite needs to be hands-on. Prepare them. Once you've done that, you have a partner, an ally, for dealing with the challenge."
>
> **— Vitor De Souza, Vice President of Global Communications, FireEye Inc.**

Second, breaches often occur over long periods of time. The median amount of time adversaries of Mandiant clients spent inside the perimeter before detection in 2015 was 146 days, according to the Mandiant report *M-Trends 2016*. "If you find it on day five, there's only so much damage that can be done in that time," Kawalec says. But sometimes breaches aren't discovered for months, or even years. Long delays in detection make the crisis far more difficult to manage—and to explain to various affected audiences. The questions asked in the wake of a breach—such as why it took so long to discover the breach, and why it happened in the first place—have the potential to be much more damaging to a company's reputation than those typically asked after a fire or other natural disaster.

Even so, Kawalec and other experts say it's critical to keep stakeholders informed following a breach. "The worst thing is rumor and conjecture," Kawalec says. "Create a framework for answering questions honestly and with integrity. Be transparent about what you do and don't know."

53%

Percentage of breaches discovered from external sources such as law enforcement, media, customers, suppliers, or even attackers themselves

Source: *M-Trends 2016 Report*, Mandiant, a FireEye company

Communicate Continuously—and From the Top

Chris Leach, chief technologist for HPE Security Services and a former chief information security officer (CISO) for a large corporation, agrees. "Communicate with people upward and downward, and communicate continuously," he recommends. "Include what you know to inspire confidence that you, as a company, are addressing the issue and protecting the information." Where possible, commit to action: "For instance, say 'we're going to have this resolved by'—and then fill in the blank." Promise updates when there's more information to share.

However, Leach recommends sharing information on a need-to-know basis: "We typically would not communicate all the details of a breach to all employees," he says. "We'll only share enough to make sure they're confident that we're handling it, and that this is information they could, and should, share with their customers."

At the same time, it's important to address employee concerns about whether their own personal information has been compromised, Kawalec says. Employers typically hold sensitive data about employees: salary, address, employment background, work-performance records, and other personal details. For that reason, Kawalec says, "Your employees need to feel that you are communicating with them and that they understand what's happened."

All three experts emphasize the importance of involving the company's top leadership in the crisis-communication plan not just during a cyberattack, but also well before. "A breach is not an IT problem," De Souza says. "It's a business problem. The C-suite needs to be hands-on. Prepare them. Once you've done that, you have a partner, an ally, for dealing with the challenge."

In addition, smart organizations embracing the digital-transformation journey view their cybersecurity crisis-communication plan as a perpetual work in progress, updating it to reflect the never-ending evolution of new threats. One example

of an emerging threat: "ransomware," which an attacker restricts access to a computer system until a company forks over a hefty blackmail fee. In one high-profile incident in February 2016, a ransomware attack blocked employee access to computer systems at Hollywood Presbyterian Medical Center in Los Angeles. The cyberattackers demanded that the hospital pay the equivalent of about $17,000 via the Bitcoin virtual-currency system to obtain the decryption key for unlocking the systems. "In the best interests of restoring normal operations, we did this," hospital President and CEO Allen Stefanek wrote in a letter posted on the hospital's website.

> **"Communicate with people upward and downward, and communicate continuously."**
>
> **— Chris Leach, Chief Technologist, Hewlett Packard Enterprise Security Services**

Stefanek's letter noted that the Hollywood Presbyterian cyberattack didn't compromise patient care and that, as far as the hospital could tell, the attackers never accessed employee or patient information. But the ransom concept unnerved leadership teams in other organizations worldwide. "What if your systems come down because someone asks you to pay $1.5 million?" De Souza asks. "Are you prepared to deal with that?" Equally important: What will you say about it—and does your communication plan address such a scenario?

Build a Strong Foundation

Of course, crisis-communication plans will vary widely from organization to organization. But the experts offer a few recommendations for establishing an effective crisis-communication framework:

- **Create a cross-functional communication team.** "We had an HR person. We had communication and legal people, and someone from the IT team," Leach says in describing the cybersecurity crisis-communication team at his former employer. Based on the type of breach, the core team sometimes brought in other in-house specialists. "So it might include a storage specialist, or a specialist from a line of business in another region of the world," he explains.

- **Establish a clear leadership structure.** "When things happen, they happen fast," De Souza says. "The communication tree needs to be well-defined, with an owner who is comfortable with taking charge."

- Speak with one voice. That doesn't necessarily mean using a single spokesperson. Instead, it means ensuring that everyone empowered to speak with stakeholders shares the same message. "In all of our communication, there were only two or three people who were allowed to speak for the company," Leach recalls. He recommends providing those spokespeople with professional media training—again, well in advance of their need to use those skills.

- **Have communication platforms ready to go.** "People aren't used to managing a crisis at the speed of Twitter," Kawalec says. If the breach becomes public, put a dedicated website online as quickly as possible. Set up multiple two-way channels so that stakeholders—employees, customers, partners, the media, and others—can contact the company with information or questions.

- **Practice, practice, practice.** De Souza recommends running "tabletop exercises," regular rehearsals involving communication strategies for responding to different types of cyberattacks. How regular? Souza says in the best examples he's seen, organizations run drills every quarter and include the C-suite as well as the crisis-communication team. "You need to make sure the communication plan is operational and you can actually use it," he notes.

Look to External Expertise

Of course, many organizations lack the in-house resources needed to create, practice, and continuously update comprehensive crisis-communica-

> "The worst thing is rumor and conjecture. Create a framework for answering questions honestly and with integrity. Be transparent about what you do and don't know."
>
> **— Andrzej Kawalec, CTO, Hewlett Packard Enterprise Security Services**

tion plans, especially given the sheer diversity of potential cyberattack scenarios. In those cases, it makes sense to turn to outside partners with strong experience in establishing crisis-communication blueprints and best practices. One example: HPE Security Services and FireEye, which have provided incident response, compromise assessment, and threat-detection offerings to thousands of clients worldwide, and also offer plenty of time-tested advice on planning for crisis communication.

"It's clear that you can't control the communication cycle without having done some work in advance," Kawalec notes. "So ahead of time, we can develop with you, or for you, a very well-thought-out crisis response plan with different blueprints and scenarios. Then we use that as a training manual that your teams can use to operate in real time."

That way, when the inevitable occurs, organizations are well prepared to respond, Kawalec says. "In the heat of the moment, you know what to say and how to say it. You know how to articulate different messages to different audiences. You can take control of the situation and communicate it out."

To learn more about digital transformation and cybersecurity, please explore this HPE-FireEye resource website.