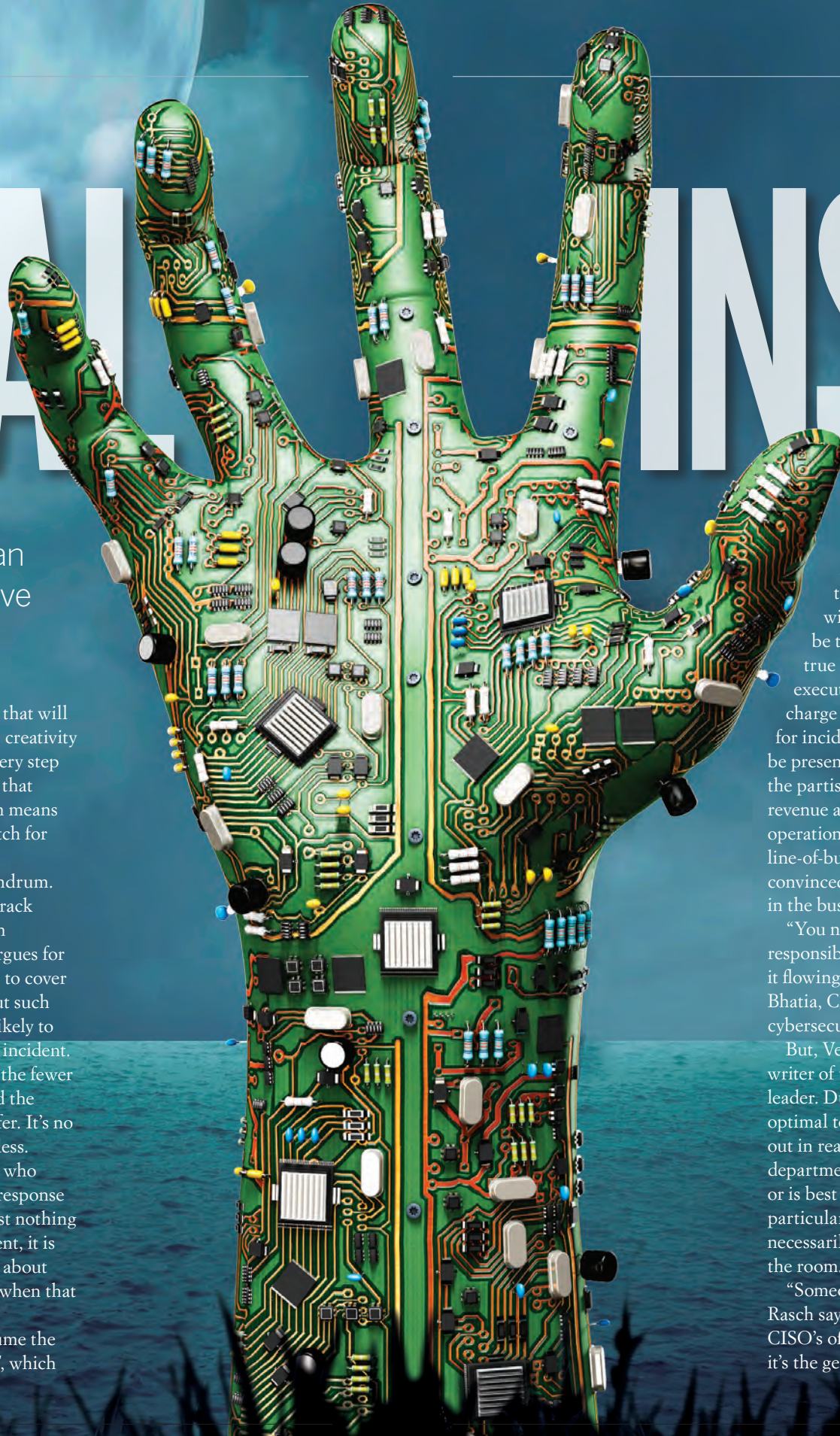


SURVIVAL INSTINCT



Some believe preparing an incident response plan is a useless precaution. Regardless, we must have them. Evan Schuman reports.

There are few corporate tasks more thankless than crafting the first draft of the company's incident response (IR) plan. For sheer smile-killing drudgery and political quicksand, it even edges out the dreaded disaster recovery plan. At least using the word "disaster" cuts the writer some slack in recommending drastic measures, a level of hyperbole that "incident" surely cannot match.

But write these incident response plans they must. What to include? What to exclude? Even more important is whom to exclude and include, when the document lists who is to be tasked with various functions.

"The goal of an incident response program is not to do the right thing. In fact, there is no one right thing," says Mark Rasch, the chief security evangelist for Verizon and a former federal prosecutor. "Your goal is to do the least wrong thing in the right way, and for the right reasons."

In discussions with data security executives who read these incident response reports by the truckload, it seems that the whom question might just prove to be top priority of the document.

The theoretical point of an incident

response plan is to anticipate things that will go wrong and to use experience and creativity to spell out in excruciating detail every step that should happen. The problem is that incidents are always different, which means the plans will never be a perfect match for whatever has happened.

That creates a *Catch-22*-like conundrum. Acknowledging that our collective track record of guessing the specifics of an unknown data breach is dirt poor argues for generic and vague suggestions, so as to cover as many eventualities as possible. But such vague and obvious suggestions are likely to be of minimal use during the actual incident. In short, the more specific the plan, the fewer situations to which it will apply. And the more general, the less help it will offer. It's no wonder that this task is often thankless.

This brings us back to the critical who issue. Given that we are detailing a response for an incident while knowing almost nothing specific about this yet-to-happen event, it is important to make the right choices about who will be in the room to respond when that event comes.

Most incident response plans assume the incident will involve security and IT, which

is reasonable. But representatives from all departments that will likely be impacted need to be there – and that is particularly true for the senior line-of-business executives. They might not be in charge – and they often should not be for incident response – but they need to be present to be the voice of the customer, the partisan who will argue to preserve revenue at all costs. And if business operations have to be disrupted, it is that line-of-business executive who needs to be convinced why, presumably because it is in the business's best long-term interests.

"You need someone in there who is responsible for the revenue, to keep it flowing no matter what," says Vikas Bhatia, CEO of the New York-based cybersecurity firm Kalki Consulting.

But, Verizon's Rasch stresses that the writer of the plan must also designate a leader. During an emergency, it is far from optimal to let executives battle this one out in real time. The chief is based on the department that is most directly impacted or is best qualified to put out this particular fire. That means it might not necessarily be the most senior employee in the room.

"Someone owns the investigation," Rasch says. "Maybe that's IT or the CISO's office. Maybe it's security. Maybe it's the general counsel or outside

counsel. Maybe it's risk or HR. But someone owns it."

While many people participate in the investigation, someone either calls the shots or coordinates the moving pieces, he says. "An IT security incident is not actually an IT security incident. It's a business incident, a regulatory incident, a legal incident, an HR incident. If you treat it as a technical incident, you will only do a technical response."

Steve Hunt, an industry analyst at Hunt Business Intelligence, agrees, adding that, sometimes, different departments can and should go their different ways. "There may be a core team, but in the moment of enacting an incident response team, people and groups outside of that core team will be affected. HR has to do what it does, so does legal," Hunt says.

"There are many different types of threats that will require unique and different responses," he notes. "A compromised database of customers requires a different response than an unauthorized wireless access point."

Many plans obscure any real direction with an overload of details, says Mark Madar, the national director for Cbiz Risk & Advisory Services. "They try to be so specific – listing out specific procedures and trying to spell out everything – that they end up overloading the plan," Madar notes. "They make it so technical that

there is no clear direction on who is doing what.”

Madar cites one particularly glaring example. “It included the specific recovery steps for a particular system,” he says. “This part of the plan only dealt with this particular ERP [enterprise resource planning] system. It was full of specific programming instructions and configuration details within that one system, rather than a framework of how to deal with these incidents. There was no clue as to how we are coming together to deal with this issue.”

What specifics would Madar rather see in a plan? “I want to see an inventory of their software and the licensing and where those licenses are maintained,” he says. In addition, he says he’d want to see lists of folders and what information is supposed to be in those folders.

Another commonly overlooked item, Madar says, is the service-level-agreement [SLA] details, including contact information. If something has gone wrong, vendor support is going to have to be one of the first calls made so the contact information and terms – are they being paid to deliver 24/7 support, for example – needs to be easily found, he warns.

On the list of pieces of information that should be in an incident response plan, but rarely is addressed, is the question that no one wants to ask: Should the business be temporarily shut down?

Tim Erlin, director of IT security and risk strategy at Tripwire, argues that a business shutdown is a last resort, but there are times when it is going to be the right move. In the heat of the moment, most will be hesitant to propose – and certainly to order or to approve – a move that will halt all revenue, give a

“You need someone in there who is responsible for the revenue.”

– Vikas Bhatia, CEO, Kalki Consulting

temporary opening to competitors and pose a severe hardship on customers.

That said, if a brief, perhaps a one- or two-day shutdown, will allow for an incident to be completely resolved and continuing operations would threaten far more permanent damage to corporate assets, that decision might have to be addressed. And, Erlin says, the calm that surrounds the writing of an incident response plan creates the best environment for a reasonable, well-thought-out articulation of when

shutdown is the preferred route. “It needs to consider, in writing, when the business really should be shut down,” he notes.

However, Hunt questions whether a report really should address shutdowns, primarily because there are an infinite number of variables that have to be dealt with by management

at the time. “Besides, there’s no such thing as shutting a business down,” Hunt maintains. “You can shut down the servers, but the business remains the business, customers remain customers.”

A less dire suggestion, Erlin suggests, is to continually reassess the plan’s threat modeling, the lengthy list of assumptions that all of the recommendations are predicated on. “Assumptions sometimes fail the threat model,” he says. “People make them at the beginning of the process and never review them.”

Of course, not all plans are the result of hundreds of hours of hard work.

Kalki’s Bhatia recalls one recent plan that sounded to him really familiar. The plan “looked familiar. Even the reference numbers looked familiar to me,” Bhatia says.

It turns out that the plan the client submitted for his review was a direct copy of a plan used by his previous employer, Bhatia says. “That’s what you *don’t* want in there. You don’t want to find pages from the *Encyclopedia Britannica*.”

Further, Bhatia echoes Madar’s complaint that many corporate plans drown in excessive and unnecessary details. “I’ve read plans that are so detailed that it would take you forever to find out who your key contacts are,” Bhatia quips.

But, he cautions, there’s something worse than having one overly detailed plagiarized incident response plan, and that would be having 30 overly detailed, plagiarized incident response plans.

That is a serious problem as some companies allow each division, and sometimes every business unit, to come up with their own incident response plans.

That, Bhatia says, is the “worst case scenario, where you have different IR plans and different technology group plans, with all tech groups siloed.” But, he also advises against plans that overreact, citing a plan that advised: In the event of a virus outbreak, turn the server off. “That’s great,” Bhatia says rhetorically. “Let’s remove all traces of forensic evidence.”

In terms of assumptions, Superstorm Sandy gave parts of the Northeast a strong reality check into the bad assumptions of incident response plans. First, companies knew that they needed power generators so many of them kept

gasoline-powered generators in the backroom. Reality check: Gas stations couldn’t get gas and those that could were ordered to ration and to only pour into car tanks, not gas containers for generators.

Bhatia spoke of New York City incident response plans during Sandy that did not consider the scenario where all of the tunnels and bridges would be closed, sealing in whoever was already in the city. “They hadn’t taken into account the fact during Sandy that most of the people that needed to respond to the plan lived in Manhattan,” he says, adding that the recovery site was in low-lying land and therefore flooded and was unable to function.

The biggest shortcoming Bhatia has dealt with were plans that didn’t provide easy and quick access to network access credentials. “What people often forget to say: ‘Who has the credentials to do what? What do you do if those people are not around?’ This is the whole key-staff risk situation, where you have over-reliance on certain people.”

Verizon’s Rasch says he’s seen plans where management insists that his team only have access and that the credentials are only in one place. “But if we somehow lose it, I want someone else to be able to get in.” That’s one of the most daunting incident response plan challenges: Giving CIOs and other executives some semblance of what they want, even if what they want is contradictory.

Rasch offers several examples of the kind of contradictory thoughts at issue. “We want strong, powerful encryption. We want it to be ubiquitous, automatic and unbreakable. We want it to be user-defined and to serve multiple functions of protecting data in storage, in transmission and while being created. We want data to be encrypted just about all the time. Oh, and we – and we alone – want the key,” Rasch emphasizes.

“We also want the ability to quickly and easily find data across the enterprise – something we mostly can’t do if the

data remains encrypted,” he explains. “We want large numbers and large classes of users to be able to find data no matter where it exists. Again, that can’t be done if the data is encrypted. If we lose the encryption key, we want to be able to recover it and decrypt the data.”

This means having or being able to create more than one key. “If the user creates a document,” he says, “we want the supervisor or employer to have access to the user-encrypted document.”

That means a multi-party key, which is much less useful for non-repudiation or digital signature. “We want the ‘good guys’ to be able to use encryption, but keep the ‘bad guys’ from being

“Hesitation can be very costly.”

– Steve Hunt, industry analyst, Hunt Business Intelligence

able to conceal their messages. We want our strong crypto to come with a super-secret back door that only authorized individuals can use for authorized purposes. In other words, we want the impossible,” he says.

On the other hand, Rasch emphasizes that every incident is different. The incident response plan is just that: a plan of action. If the plan doesn’t make sense under the circumstances, the security teams needs to adjust it. “Just make sure that you know why you are abandoning the plan,” he says.

For his part, Hunt cautions that the biggest issue with incident response plans is that they tend to end up being all talk and no action. “The big problem that plagues most incident response plans is simply that it never goes beyond the paper,” Hunt says. “Someone creates the plan to comply with an audit.

They write the plan and they show the customer the plan. The customer asks ‘Is everyone trained and informed?’ and

they say ‘yes.’”

But what happens when an actual emergency materializes? “The incidents occur and the plan is never enacted,” Hunt says. “There is no mapping between the bad things that are happening and the actual incident response plan.”

Another concern that Hunt stresses is that the typical perfunctory training that most companies do with their approved incident response plans do little to help when the incident really happens. “You need to do more than training,” he says. “We can have tabletop exercises until their butts are numb and, still, when the times comes,

there can be more than a single moment of confusion,” Hunt notes. “Hesitation can be very costly.”

Instead, he says the principles and actions in the incident response plan must become simply a part of the culture of the business and a perfectly natural response from the relevant employees. “Until the security mechanisms are embraced and infused throughout the organization, incident response is going to be choppy,” Hunt says, citing an example of an attack that impacts an e-commerce application.

“You need authentication, authorization, administration and audit,” Hunt maintains. “Those four concepts are all seen as part of security, but the business unit management doesn’t think of them as security. They are just normal business.”

When security is treated as just a regular part of business, the incident response plan has a chance to work, he says. ■