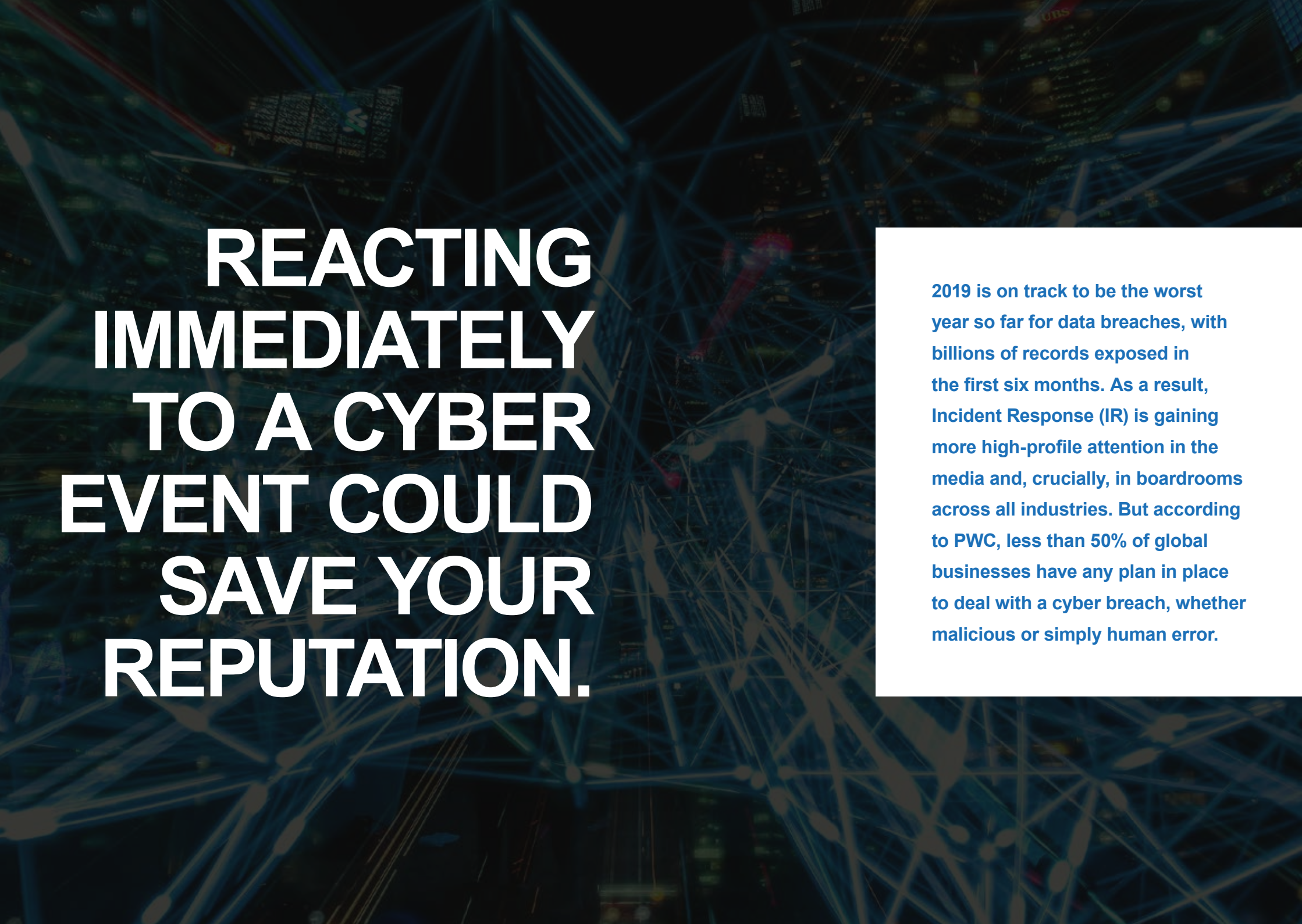
INCIDENT RESPONSE

RICHARD PICCONE

6 SIMPLE STEPS



REACTING IMMEDIATELY TO A CYBER EVENT COULD SAVE YOUR REPUTATION.

2019 is on track to be the worst year so far for data breaches, with billions of records exposed in the first six months. As a result, Incident Response (IR) is gaining more high-profile attention in the media and, crucially, in boardrooms across all industries. But according to PWC, less than 50% of global businesses have any plan in place to deal with a cyber breach, whether malicious or simply human error.

Ensuring that everyone in your business knows what to do as soon as a breach is detected is a critical priority that may save both your reputation and your bottom line. However, are your security professionals providing enough information and involving the right people to ensure management teams make sound investments and strategic decisions to shape incident response plans?

I remember once being asked if sending the IR team on a touch-typing course would be beneficial – the thinking being that they could out-type hackers during an attack. The joy of epic keyboard battles notwithstanding, it was apparent to me that the reality of incident response (and sometimes IT in general) hadn't been made clear to a group of people who were key players in the process. Without naming and shaming, there are plenty of examples of public relations faux pas (to put it mildly) in the time following a major security incident, and they all demonstrate the importance of keeping your Top Brass informed. This article will give you a primer on a typical incident response process, which will hopefully add more context to what your public relations team may tell you to say, or why your technical team have locked you out of their office!

The anatomy of Incident Response

The incident response process can be described as having six phases:

Phase 1: Prepare

As you might imagine, this is the phase that requires the most attention and effort. Good preparation needs all areas of the organisation to contribute, and this process should be led by senior management, as the incident response process will either be dictated by, or dictate new, business processes. Preparation will involve everything from defining roles and responsibilities, to deciding a communications strategy, to implementing uniform and thorough log collection on your computing and network infrastructure. Remember the old adage: "Fail to prepare, prepare to fail". In reality this is actually a continual process, so part of your initial preparation should be to define suitable processes by which you can onboard new systems and review measures for existing ones.

You should seek assistance here too; getting expert help to check how prepared you really are, and to seek out any gaps in your defences will pay dividends in the long run. The cyber threat landscape changes on a daily basis and reaching out to recognised experts is always a good option. You can also invest in cyber insurance or subscribe to a recognised incident response service, these are good options when you may not have the internal resources to handle a cyber event.

Phase 2: Identify

This phase is relatively short, but decisive, and is where the preparation starts to pay off. With this being the first 'live' step in the incident response process, it's vital to start documenting everything being done. Your preparation should have included a standard format for documentation, and it should start with the basics; who's handling the event, what time the event was first reported, what systems are affected, etc. Your responders will then start working through a predefined checklist to determine the state of the affected systems and compare them to an established baseline for what's considered normal. (Notice that I've been using the word "event" rather than "incident"; part of your preparation should be to define what actually constitutes an incident and, until it's confirmed that an event meets those criteria, it's still just an event.) During this phase, responders will use the information gathered to determine the next steps, which may be to downgrade the event and exit the response process, monitor the event for a period of time to gather more data, or declare an incident and escalate.

Phase 3: Contain

If you reach this phase, it's because you have an incident in progress. The natural response is to immediately try to contain the problem, but in order to do so effectively you must first confirm what type of incident you're dealing with. While it may seem counter-intuitive that this isn't performed during the 'Identify' phase, remember: during that phase you're identifying the nature of the event, not the type of incident. A Distributed Denial of Service (DDoS) attack, corporate website defacement, and an unauthorised employee accessing sensitive corporate records are examples of potential incidents. Each of these examples warrants a very different response, so effective action requires effective classification of the incident. Likewise, incidents of some types might require notification of other parties, such as senior management, partners, customers, or even government bodies. Again, this will have been covered during your preparation phase, along with suitable immediate actions, such as disabling accounts, blocking traffic at the firewall, and so on. These actions come with risks and making a wrong decision could make matters worse, rather than better, so think about them carefully beforehand. An example of a poor response would be pulling the power on a compromised machine – it destroys valuable evidence and, while it may stop the incident in progress, the machine can't be investigated while it's off. Instead, it would be better to isolate the machine in a non-invasive way, such as blocking traffic at the firewall, so that malware can't spread to other devices. This is important because it's at this point that your responders will collect volatile system data, such as memory images, so the actions they take will do as little to upset that state as possible. Once your responders have confirmed that the incident has been contained, the process can move on to the next phase.

Phase 4: Eradicate

The incident cannot progress beyond this point, so it might not be until now that you can get much information from your responders. I can tell you from personal experience that having the CTO and CEO breathing down your neck while you're trying to stop an incident is counterproductive; let your responders work and they can give you a more meaningful update during this phase. It's now that the hunt begins for the root cause. The type of incident will dictate how to go about this, but an example would be finding an attacker's malware implant on a machine, ensuring it's copied in a forensic image, then restoring the machine to a known good state and tackling whatever vulnerability was exploited (e.g. installing missing patches). The last step in this phase is to run full analysis across all systems to ensure the vulnerability doesn't exist elsewhere – assume it does, and assume the attacker already knows that.

Phase 5: Recover

Once the hole has been plugged and everything has been returned to a safe state, you're ready to resume BAU activities. It's prudent to continue more stringent monitoring during this phase, rather than standing-down immediately, in case of any repeat events. For instance, a DDoS attack may be a precursor to, or a distraction from, a network intrusion, which you'll be in a better position to find and eliminate if you're scrutinising your network logs more than usual.

Phase 6: Follow up

As much as you might want to wash your hands of the whole ordeal, the follow-up is just as necessary and important as the preparation, as it closes the loop. This is where the documentation and analysis pay dividends, as this phase is all about lessons learned that feed back into your IR preparation. Likewise, the documentation should be reviewed, written-up in a report, and safely stored as important reference material for any future incidents, or even regulatory audits.

Conclusion

As you can see, even describing the phases of incident response at a high level is quite involved – I could do an entire series on the preparation phase alone – but the benefits of having a solid plan in place far outweigh the hardships of getting there, because you can quickly regain control of a potentially dangerous situation. Ever the stoic, I'll paraphrase Kipling: "If you can keep your head when all about you are losing theirs . . . yours is the Earth and everything that's in it."

PHASE 1: PREPARE

In the previous article, I described the six typical phases of an incident response process. After posting it, I was approached by several people asking for more information, so I've decided to expand my original article into this series covering each of the six phases.

To begin, I'll address the second most common question I was asked: "How do you know you've done enough preparation?" There is a straightforward, if rather glib, answer: you don't. What this is alluding to is that preparation for incident response is a continuous exercise. In reality, you'll only know you've done enough when you can run through incident response drills without coming unstuck in your scenarios. At that stage you should still revisit your plans periodically, to ensure all the elements are still relevant and effective.

The bulk of this article will, of course, be to address the question I was asked more than any other: "Where do I start?" As with many other aspects of cyber security, I like to break this down into three key areas: People, Process and Technology.

People

Getting the right people might sound straightforward enough, but good incident responders have specialist skills and experience that you probably don't already have internally. However, in the early stages it's better to source reputable third-party specialists who can help get your incident response capability off the ground, rather than try and recruit your own talent. You'll also want to define roles and responsibilities for everyone from the board level down. Everyone has a part to play – from the CMO authorising press release statements, to specialists performing digital forensics, to entry-level staff reporting the events that trigger the IR process. Knowing you can rely on your people removes an enormous amount of the stress from an incident scenario, so you'll want to invest in your teams; set aside a realistic budget for ongoing training, including your helpdesk (they'll be performing the initial triage of events). At the same time, review the cyber awareness training you provide to all staff – is it enough? Will it complement your carefully crafted incident response plans?

Process

Your internal policies and procedures should complement your incident response process, and you might find you need a lot of work in this area. Some examples would be alterations to HR policies that support and protect your incident response team during their investigations, or a statement in your employment contracts that informs staff of the incident response team's right to access and monitor corporate devices. You will also need to write policies specific to the incident response process - here are some common examples: incident categorisation, escalation processes, service level agreements, communication policies (who/what/how/when to notify shareholders, media, law enforcement and regulatory bodies), the criteria for response actions (such as monitor, quarantine, pull the plug, etc. Include fixed time frames, as well as threat intelligence and risk factors), evidence collection and handling methods, incident response drills and system readiness checks. Your incident response capability can (and should) feed into your business continuity and disaster recovery plans, so you should review them to ensure they can be triggered effectively by an appropriate incident response process outcome.

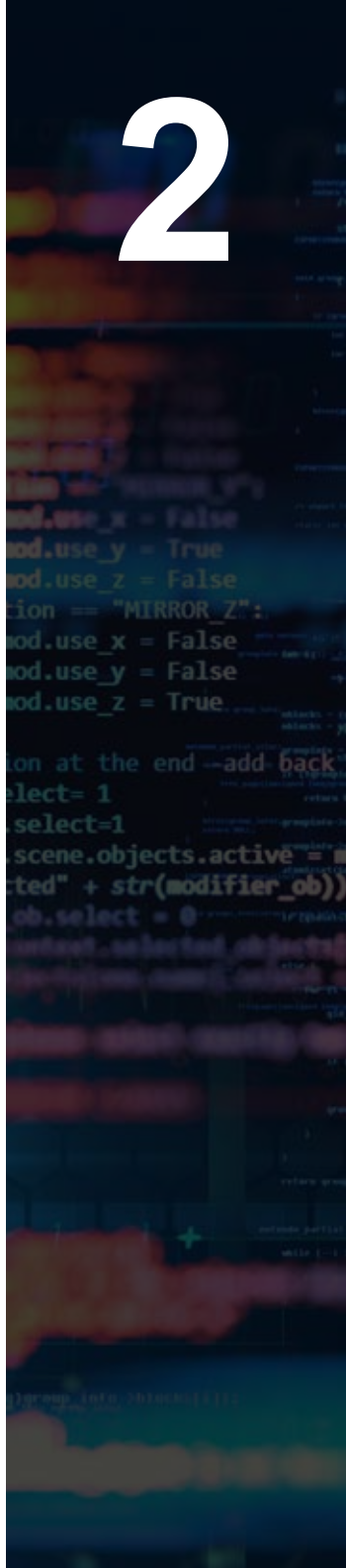
Technology

This is the area that will require the least amount of input from senior stakeholders, but you should be prepared to review budgets if you're missing key IT resources. Important technical considerations are to ensure you have sufficient logging enabled on all critical devices; the amount and type of logs will vary from system to system, but they should be stored in a central location and subject to strict access control and backup policies. An often-overlooked consideration is ensuring accurate timekeeping across your network by using correct Network Time Protocol (NTP) configuration; this is especially important when correlating events in logs across multiple devices, which becomes increasingly more difficult with inconsistent times on your machines. Other technical requirements are ensuring consistent and secure Access and Identify Management (AIM) throughout your network with accompanying policies; for example, ensure that you do not use shared accounts, and have a "one person, one account" policy where feasible. Be clear and consistent with naming conventions, as these will be reflected in logs and deciphering obscure or inconsistent user and host names will only hinder the incident response team's efforts. Make the effort to comprehensively document all systems on your network, along with copies of running configurations, clear network diagrams, and a baseline for what 'normal' network behaviour is. This will greatly aid your responders throughout the process. Your responders will also need dedicated equipment, such as secure laptops, servers and data storage for the purpose of triage, diagnostics, and digital forensics. You should also consider giving them a means of out-of-band communication, i.e. communication that does not rely on the potentially compromised network, such as mobile phones. Don't be surprised that some (or all) of this equipment sits untouched in a secure area; it may look like an expensive way to collect dust, but it's important that your responders have 'clean' kit readily available so they can focus on the task at hand, rather than scrabbling for cables and spare hard drives, or troubleshooting their laptop before they can deal with the incident.

Conclusion

As I mentioned in my original article, I could write a whole series just on preparation alone. Every environment is different, with its own quirks and requirements, but the thing they all have in common is that their administrators need a plan and resources for when things go wrong – how much you give them will depend on how much you're willing to lose! Hopefully this more detailed look at incident response preparation has whet your appetite for what comes next: alarms are ringing, lights are flashing and eyes are widening - is this a false alarm, or do you have an incident on your hands? Find out how you can tell in my next instalment!

PHASE 2: IDENTIFY



In the first article of my series on Incident Response I covered the key areas you should consider when preparing your incident response capability; this instalment will look at what happens when those plans get set into motion.

First, I want to clear up some important terminology:

- An **event** is observable behaviour that deviates from the established norm. Some examples of events are an error message on a server, a change to firewall rules, or a user logging in outside of their working hours.
- An **alert** is a notification that an event has taken place.
- An **incident** is an event or series of events that negatively impact the confidentiality, integrity or availability of your data. Some examples of incidents are a ransomware outbreak, a user transferring privileged data out of the network, or a loss of power to the server room.

The definition of an incident really depends on the organisation's risk appetite and incident response capability, as well as the specific information system in question. However, the definition I've provided is focused primarily on the protection of data which, now more than ever, is crucial to any organisation. I'd like to walk you through a simple scenario to illustrate this phase of incident response, and I want you to think about how your teams might deal with this in line with your own risk management strategies.

One of your technical teams notices a high number of "404 Not Found" errors logged on your web server. This error is not unusual and is typically caused by a user mistyping an address or trying to access a page that doesn't exist, like a deleted blog post. However, the team also observes that a high number of errors occur within a very short space of time, come from the same IP address, and the requested pages have names such as "login.html" and "admin.php", which doesn't fit the usual pattern of activity for this system. This leads your team to the conclusion that there is a high probability an attacker was attempting to use brute force guessing to find login pages.

> *Tools such as Security Information & Event Management (SIEM) platforms make tasks like this much easier, as they can provide real-time analysis and correlation of such events and automatically generate an alert, allowing your team to react sooner and conduct more efficient investigations.*

During their investigation, your team observes the suspicious IP address finding your website's admin login page, and they decide to check the access logs, where they observe a similar pattern of numerous failed login attempts, followed by a successful login.

> *Public-facing administrative tools are a common misconfiguration and should be highlighted in vulnerability and risk assessments. Typically, access to these tools can be restricted to only be allowed from inside the corporate network; if this was the case, this incident response scenario would likely stop here, but that doesn't make very interesting reading!*

For final confirmation, the team geolocates the IP address to a part of the world where you don't have employees, and the marketing department confirm that none of them had logged in that night to make changes to the site.

> *System logs aren't the only source of useful information for your incident response team – knowing that an employee is on leave, for example, can steer an investigation in the right direction, so this is why it's important to facilitate access to this sort of information (in a controlled manner) during your preparation phase. Automated tools that employ User Behaviour Analytics (UBA) work in conjunction with SIEM platforms and boost the capability of your incident response team.*

Now it's clear that these events constitute an incident, as there was unauthorised access to your systems, which puts the safety of your data in jeopardy. The team document everything and two team members are assigned as incident handlers – this allows for a "two sets of eyes" approach to the investigation and response, and also allows one responder to take a hands-on role while the other concentrates on documentation, making for a more efficient process.

> *There are ticketing systems typically used by IT helpdesks that will be of immense help to your team, as they'll allow a central place to accurately record the pertinent information. Many of these can also be integrated with SIEM platforms, allowing for more automation and increasing the productivity of your team.*

There you have it: your team have been alerted to suspicious events, they've calmly followed a methodical and systematic line of investigation and determined, according to well-defined criteria, that there has been a security incident. The proverbial wheels are in motion, but what happens next? Find out in the next instalment, where we start the Containment phase!

PHASE 3: CONTAIN

In Phase 1 we looked at how to prepare your incident response capability and in Phase 2 we looked at how that preparation paid off, as we walked through a scenario to identify a security incident. Let's continue the scenario and contain the incident.

To recap: the incident response team received alerts of suspicious events on a web server and, after some investigation, found that an attacker has managed to find the admin login page and guess the credentials.

The first step in this phase will always be to categorise the incident, as the type of incident will dictate the actions you take next. There are a number of frameworks you could use to classify an incident, an example of which being MITRE's CAPEC framework. Using that example, this incident is classified as CAPEC-16: Dictionary-based Password Attack. The team come to this conclusion by checking the password for the compromised account against commonly-used wordlists and finding a match.

> *A wordlist is a file full of words or phrases that are typically used for passwords; a famous example is called **rockyou.txt** and contains over 14 million entries of passwords that were (and still are!) in active use. While there are common wordlists available, an attacker can also create a custom wordlist that more closely relates to their chosen target (containing variations of the organisation's name, for example). Using long, random and complex combinations of characters effectively defeats these dictionary attacks.*

Having classified the incident, the responders can now take the prescribed immediate actions; they change the compromised password to a random, complex password 20 characters long and store the new password in the company's password manager, which has an encrypted database and an audit trail for logging access to credentials. This will prevent the attacker from using the compromised account any further.

> *In this case (and in many others) it would be unwise to consider options such as quarantining the machine or pulling the plug entirely, as this would cause disruption to the business and potentially destroy important evidence, but provide little gain.*

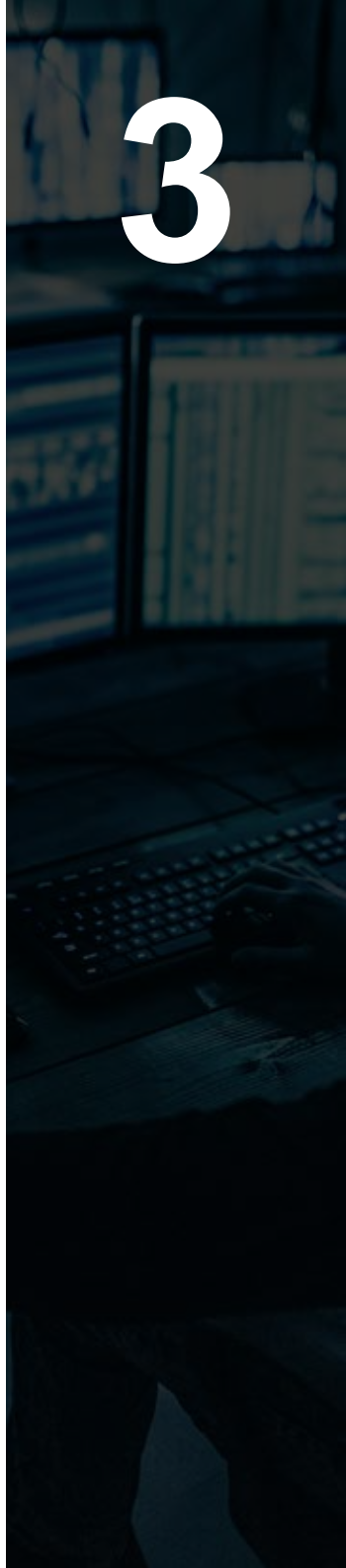
Before moving on, the team checks the access logs for any connected systems to try and correlate events and determine whether the attacker moved through the network to establish a persistent presence. For the purpose of this scenario the web server is standalone, and the network logs show no connections from the web server to the internal network after the compromise. They implement more detailed monitoring of the network traffic to and from the machine, in order to catch any traffic that would indicate the attacker's presence, and send a brief to the senior management team to outline what has happened so far and what the proposed next steps will be.

> *As senior managers, it makes sense to get an update at the close of this phase, but not before; this is where your team can provide you with meaningful, actionable information that enables important business decisions (such as whether or not to notify other stakeholders, regulators, etc). If you get notified of every event, you'll become fatigued very quickly; if you're notified that an incident has taken place but don't know anything more, you're left with uncertainty, and might be tempted to press the team for updates prematurely, interfering with the process.*

While reviewing changes made by the compromised admin account, the team find the attacker created a second user account, and a hidden page called "shell.php", which provides a means for the attacker to interact with the server without logging in. After removing these artefacts, the team are satisfied that the incident is contained, as the attacker has no means of unauthorised access to the web server or other systems.

There are many other considerations to make during this phase. For example, it's best to take a forensic image of the compromised system before making any alterations, in order to preserve the compromised state for evidentiary and investigative purposes. Another consideration is whether you want to make changes that would alert the attacker to your presence – in some cases, it might be better not to tip your hand right away. These sorts of decisions depend on the nature of the incident and can have specific technical requirements and consequences, which is why it's best to involve seasoned incident responders during your preparation.

Thankfully, the situation is now under control, and your team can press home their advantage. It's time to eradicate the attacker's presence on your network as they move on to the aptly named Eradicate phase!



PHASE 4: ERADICATE

So far, we've looked at the first three phases of a typical incident response process: Prepare, Identify, and Contain. To illustrate the more active phases of the process we've been using a scenario in which an attacker has found the administrator login for your web server, guessed the login credentials, and created a new account and a secret web page to give themselves access to the server. We've looked at how your team has received an alert and investigated the events to confirm there's an incident. In the last instalment your team categorised and contained the incident, and implemented monitoring to catch any further suspicious activity.

The task now at hand for the team will be to ensure the attacker's presence has been eradicated from your systems. It may seem like this was taken care of in the last phase, as the team changed the administrator password and removed the tools the attacker installed to maintain their presence and, in the case of our scenario, that's largely correct. The same generally applies if you catch a similar incident early enough in the real world. However, you don't simply drive the enemy back and hope they don't attack again; as I stated at the end of the last phase, it's time to press your advantage and make certain you can't be attacked again. Let's see what that means for our team.

The team start by performing a root cause analysis to identify the means by which the system was compromised. This is simple enough for this scenario: an easily guessable password on an administrative account.

> *While it's simplified for this scenario, in reality a root cause analysis could take a long time and shows why it's important to take a forensic image of the compromised machine(s) during containment before making any changes. There could be a complex series of steps involving a combination of known vulnerabilities and misconfigurations that allowed the attacker to gain access; it takes time and skill to pick this apart but, once finished, your team should be able to replicate the attack and determine what needs to be fixed.*

This aids the team in another important investigation: they know that the attacker was attempting to establish persistence on the web server, so they use the information gained from their analysis so far to determine whether the attacker was able to install a rootkit on the machine.

> *A rootkit is software used by an attacker to enable persistent access to a compromised system in such a way that avoids detection. To this end, they're often embedded deep within the operating system and can include tools to log keystrokes or read passwords from memory. Due to the way they're installed, often the only recourse is to completely wipe the machine and reinstall the operating system and software, which is why it's important to find them early, because this can be a very disruptive process to the business.*

The team concludes that the attacker only had access to the website's content management system (CMS) and, in this case, this wouldn't allow the attacker to write files to the filesystem beyond the scope of the website's content. In other words, the attacker couldn't use the website administrator account to install programs on the server; they could only create a web page and a new CMS user account.

> *This is why it's important to follow best practices when building key systems, especially those that are public facing and exposed to attack. If the CMS had been installed incorrectly, the access may have been too permissive and allowed a low-privileged CMS user to modify the server's operating system. This also highlights the need for role-based access control; even if you're the administrator of the website, that doesn't mean you should also be the administrator of the web server.*

The focus for the remainder of this phase is to harden defences and ensure this type of compromise can't be repeated. The team have already created a more secure password for the admin account, so they initiate enhanced user awareness training for the users of that system. They also implement an account lockout processes to prevent brute force guessing of users' passwords, and decide it's preferable to use named accounts with delegated roles instead of the default administrator account. The team review the permissions of system accounts to ensure website CMS users can't write to the filesystem outside of the appropriate scope and, finally, they change the web server's configuration to include two new features: rate-limiting to prevent a high number of requests in a short space of time, and access rules that only allow access to the admin login page from the internal corporate network.

The final step should be to perform a vulnerability analysis to find any further weaknesses; the one our attacker found might not be the only one, and the changes we've made might have inadvertently created a new vulnerability. Once this is complete, the incident response team can be satisfied that the compromised system is now secure and will issue another notification to this effect.

With that having been said, now's not the time to rest on our laurels! As you'll know, there are still two more phases to this process, and I'll cover those in the next instalment.

PHASES 5 & 6: RECOVER AND FOLLOW UP

So far, we've look at how to prepare your incident response capability, and I've taken you through the live steps of an example incident, which has now drawn to a close thanks to the sterling efforts of your theoretical team. What more is there to write about? Honestly, the final two phases probably don't warrant individual articles, so I'm covering them both here. But that's not to say they're not important. Quite the contrary, in fact, because these two phases are the means by which you measure the success of your incident response programme.

Phase 5: Recover

This phase can be relatively short, depending on the incident. In the example of our scenario, we didn't discuss taking any systems offline, but during this phase your incident response team would coordinate with relevant departments to bring systems back online after testing and verifying that they're performing correctly; it's the time when things are truly returned to business as usual.

It may be necessary or desirable to monitor the affected systems more closely for a fixed period – something that should be determined during your preparation – or you may find that you make a permanent change to your existing monitoring. In the case of our scenario, an example might be generating a system event log each time a web page is created. These changes are highly contextual, as they're based on the type of incident, the type of information system, your logging and monitoring capacity, and so on. These aspects can (and should) all be discussed at length during the next, and final phase.

Phase 6: Follow Up

This is the phase where we analyse the incident in retrospect, and absolutely should involve senior management because it will result key business decisions being made. The incident response team will write a full report of the incident, starting with an Executive Summary and going right the way down to the fine technical details, and it's the job of everyone involved in the subsequent meeting to look analyse the incident and determine what lessons can be learned from it. How did it happen? Could it have been prevented? Could it have been discovered sooner? What impact has this had on our business or our customers? Now is the right time to be asking and answering these questions, because it's only now that the full extent of the incident can be reviewed in detail. Some decisions that might result from this phase are changes to internal policies and procedures, including more user awareness training, better logging and alerting, or an upgrade to better software services. Another result is that you find the preparations you made for that system weren't enough, and this gives you the chance to plug that hole. You can see, therefore, that this phase is probably the most important of all, because it feeds back into Phase 1 and closes the loop, giving you continuous improvement through a robust incident response process. Finally, although it should go without saying, this phase should close with you thanking your incident response team; they've probably been awake in the small hours, away from home for extended periods, and working diligently to protect your business. They may be the bearers of bad news, but they're also the ones who've repaired the damage, and a "thank you" goes a long way!

Modern businesses rely on technology and data, so to run a sustainable business you need to have a strong, scalable means to protect and maintain those assets. I sincerely hope you've enjoyed reading this series as much as I've enjoyed writing it, and that you can take something away from it to improve your own use of information technology! Thank you.

Making the digital world a safer place to do business

ITC SECURE

itcsecure.com

10th Floor, 5 Churchill Place, London, E14 5HU, United Kingdom