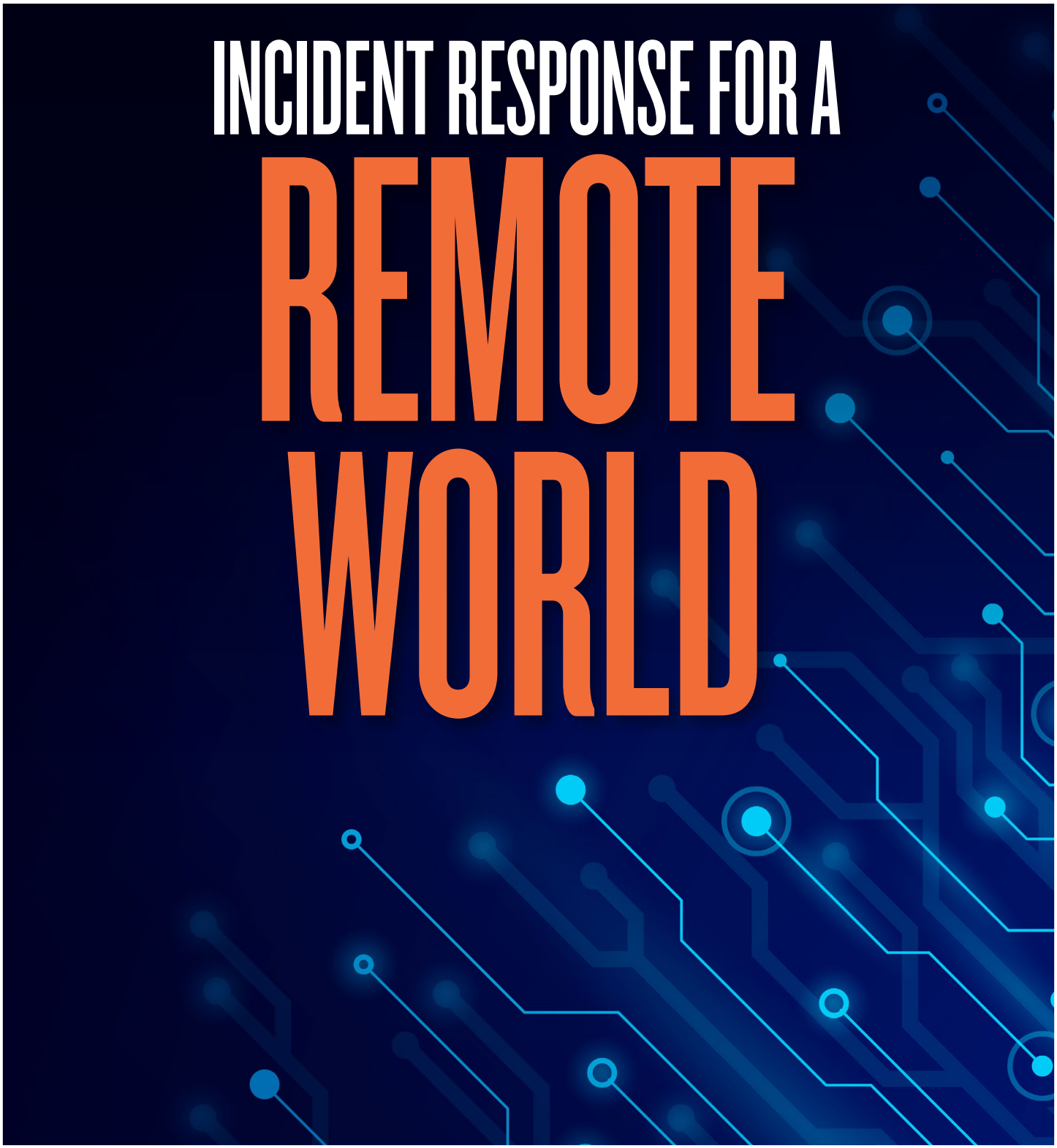
exterro

ExpertFocus

March 2022

Brought to you by Exterro



Incident response for a remote world.

Bob Violino explores the incident response challenges created by the pandemic and how organizations can adapt their IR to fit a hybrid and remote work environment.

Many aspects of the IT infrastructures that serve organizations today are nothing like they were two years ago. Hybrid and remote work models are now firmly in place at numerous companies, and they are unlikely to go away any time soon.

In the current environment, end-user devices are just as likely if not more so to be operating off the main corporate network as on it. While this creates a lot of opportunities in terms of worker flexibility, it also introduces a host of cyber security risks.

Most enterprise incident response (IR) plans were developed and put in place before the pandemic and shift in work models. They were designed for a world in which incident responders did their work on site. With more security practitioners working remotely, procedures, tools and techniques that worked well on premises no longer cut it. A new approach is needed.

In the following pages, we examine the cyber security and IR challenges created by the pandemic, the new work models that have surfaced, and offer guidance on how organizations can adapt their IR to fit a hybrid and remote work environment.

Risks Of Going Remote

Little did security leaders, their teams and organizations realize how much things were changing in early 2020, when the pandemic forced lockdowns and a sudden shift to remote work. Essentially overnight, millions of employees were relocated from corporate to home offices, drastically changing the dynamics of network access, device usage, and cyber security protocols—among other factors.

Fast forward to 2022, and remote work has not gone away — even as the pandemic is easing in many parts of the world. In fact, it has become part of the new hybrid work model that seems to be here to stay for many types of organizations.

"I think it's becoming fairly clear that this is the way it's going to be for the foreseeable future, with regards to remote work and hybrid work," says Justin Tolman, forensic evangelist at Exterro, a provider of legal governance, risk, and compliance (GRC) software. "Things have changed pretty much permanently."

This new workforce model presents several challenges for security teams. For instance, remote workers might be using their own personal devices and their own networks, which might be less secure than what their organizations require in terms of minimum protection.

"The attack surface has changed," says Arthur Treichel, CISO at Maryland State Board of Elections. "If a remote workforce is working from untrusted networks and devices, there is less visibility into the networks, endpoints, and cloud services holding critical data. That means notification or discovery of malicious activity may come later, after more damage has been done."

The fact that many employees are no longer working behind the company firewall with fully updated, company-owned devices means there is a lack of direct control that was not an issue pre-pandemic, Tolman says. Like many other companies, Exterro had some remote workers accessing networks and data long before the health crisis.

"The move to mass work from home has extended the environments in which incidents occur to remote networks, which tend to be much less secure and where IR teams have less visibility."

– Bradley Schaufenbuel, vice president and CISO, Paychex

But it wasn't as normal as it is now, and companies that traditionally haven't been working from home are now having to deal with that.

"The move to mass work from home has extended the environments in which incidents occur to remote networks, which tend to be much less secure and where IR teams have less visibility," says Bradley Schaufenbuel, vice president and CISO at Paychex, a provider of financial and human resources software.

When you factor in home networks and personally owned devices, the attack surface has expanded significantly, making the job of incident responders even more difficult than it already was.

Traditional network monitoring tools provide less utility in cases where most activity is now "off network" or does not occur on trusted internal/corporate networks.

"Without enhancing endpoint visibility, incident response teams can be left blinded by the shift to work from home," Schaufenbuel says.

In addition, in many cases security team members themselves are working in different, remote locations, which can make it more challenging to perform tasks.

Collaboration between incident response team members has become more difficult, Schaufenbuel says. Without physical war rooms, interaction between team members must be replicated within online collaboration tools, which have their limitations. For example, it's difficult for team members to have side conversations, or to have a free-flowing conversation without interrupting others.

One of the key questions for security leaders and teams is how to handle IR when devices are not even on their central networks. Effective IR is less of an issue when users' devices are connected to company networks, or when users are connecting through a virtual private network (VPN). When devices are not necessarily on the network or not using a VPN, such as when people are working from home, airports, hotels, coffee shops or other locations, IR can be far more of a challenge. At any given time, organizations might not know for sure where their remote workers are working, which devices they are using or what they are trying to access.

"Because they may be connected to a Starbucks Wi-Fi or their home network may get compromised, you're securing against risks that you didn't previously have to go up against," Tolman says.

One of the risks of the hybrid model is that employee devices and company data might be in transit at virtually any time. Someone could be working on a highly sensitive project and moving the device and its data from the company office to home multiple times a week.

Evolving Threats

Even as cyber security leaders and teams try to address the issues of remote IR, the threats and vulnerabilities continue to evolve and expand. The types of cyber security attacks have broadened since the beginning of the pandemic to include home workers. Phishing attacks are aimed at people working from home who might be less prepared or less inclined to deal with them, for example.

"There are constantly changing threats," Tolman says. "Like in 2020 we had all those instances of phishing attacks that were Covid-focused and were causing problems for people working

"Because they may be connected to a Starbucks Wi-Fi or their home network may get compromised, you're securing against risks that you didn't previously have to go up against."

– Justin Tolman, forensic evangelist, Exterro

at home clicking on things they shouldn't have clicked on. That's the kind of thing that can happen when you've got people working in different places than they were before."

Home-based or hybrid workers are not necessarily more reckless about security, Tolman says. But they might on occasion let their guard down when using their personal devices and networks for work. They might be more inclined to download applications or click on links they might otherwise resist.

Furthermore, with employees working from home and thus not in physical proximity to one other, they are less likely to notice or report suspicious behavior. In the office, an employee could ask their cube mate if something seemed a little off about an e-mail message, Schaufenbuel says. But that ad hoc communication does not occur as often in work-from-home situations. Incident response teams have lost at least a portion of this valuable source of intelligence.

What's also broadening is the targets of attacks. While there might be a public perception that only the largest enterprises tend to suffer serious attacks such as ransomware, the fact is organizations of any size can be a target.

The U.S. Small Business Administration (SBA) notes that cyber attacks are a growing threat for small businesses, which it says are attractive targets because they have information that cyber criminals want, and they typically lack the security infrastructure of larger businesses.

"It doesn't really matter what size of company you are," Tolman says. He cites an example of a friend who owns a car window tinting business that was hit with ransomware. "I just happened to show up and was able to recover his system, but this was just a little window tinting shop getting hit, so it doesn't matter where you're at in terms of size or type of business."

Another worrisome trend is that attacks such as ransomware in some cases are not just affecting the immediate targets, but their supply chain partners as well. Such attacks can put multiple systems up and down the supply chain out of commission for an indefinite period, wreaking havoc on markets.

All of these cyber threats come as many organizations continue to struggle to attract and retain cyber security skills.

"There's more work than there are experts" to do the work, Tolman says.

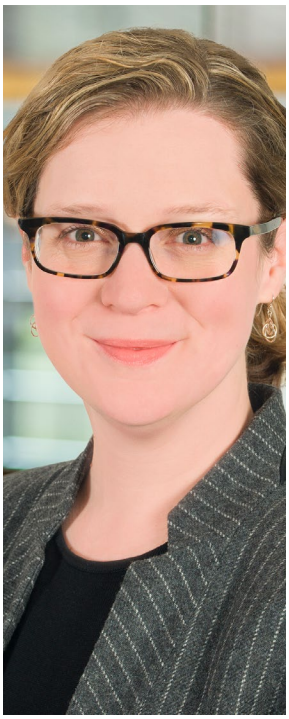
"Many companies don't have the people, the expertise that they need to deal with these challenges."

Incident Response Reboot

Developing a strategy for effective remote IR can't address all the security challenges organizations face. But it can go a long way toward helping organizations address many of the threats.

The most important thing to do to adapt IR strategies to the new hybrid environment is to understand the environment, says Jess Burn, a senior analyst at research firm Forrester.

"So many security and IT teams struggle to maintain much-needed visibility into an increasingly complex and distributed IT environment, because so much of an organization's estate is unknown or undiscovered due to cloud migration, shadow IT, [mergers and acquisitions] and third party/supply



"So many security and IT teams struggle to maintain much-needed visibility into an increasingly complex and distributed IT environment, because so much of an organization's estate is unknown or undiscovered due to cloud migration, shadow IT, [mergers and acquisitions] and third party/supply chain activity."

– Jess Burn, senior analyst, Forrester

chain activity," Burn says.

To that end, here are 10 recommendations:

1. Work with colleagues in infrastructure and operations to understand where critical data is, what protections are in place, and who has access to it.

"You should have playbooks for the most common breach scenarios, and you should be testing those scenarios often via technical and executive tabletop exercises," Burn says. "CISOs I've worked with run these exercises quarterly at the technical level and biannually" with executives.

2. Make sure devices are managed before granting access to data.

"Management will allow logging and monitoring of EDR [endpoint detection and response], authentication and data access at the endpoint, cloud services and the enterprise," Treichel says. The security operations center should be capable of ingesting and correlating data to alert the team quickly of any potentially malicious activity.

3. Deploy tools and services that provide effective incident response in a remote environment.

Technology solutions are available that allow security teams to respond to incidents without the need for direct network connectivity. They do this by placing agents on client devices.

When an incident occurs, the security team can connect with a particular device over the Internet to remediate the incident remotely. If a device is connected to the Internet, the security team can perform incident response on the device using incident response tools. This is a key capability because in many cases users might not have their VPNs turned on while they are working from home, or they might be working offsite.

These types of tools collect data from off-network remote devices, eliminating the need to ship the devices to the security team for analysis and fixes. The collected data is securely transmitted to validated servers, and security analysts can investigate incidents such as ransomware attacks, data breaches, or other threats by scanning for indicators of compromise (IOCs). They can detect and analyze suspicious activity, traffic, applications, and processes.

4. Beef up endpoint monitoring and control.

"Without the ability to rely on traditional on-premises network security controls, incident response teams need more visibility into and control over end-user endpoints

that are not always connected to the trusted corporate network," Schaufenbuel says. "Cloud-based endpoint detection and response software and user behavioral analytics agents are critical tools for incident response teams with largely remote workforces."

5. Make it easier for end users to report suspicious activity.

"The 'human firewall' is more important than ever when users are working off network, [for example], not connected to the trusted corporate network," Schaufenbuel says "Near real-time reporting mechanisms like chat interfaces to security operations teams are critical."

6. Understand how the attack surface has expanded and extend their programs accordingly.

"I would recommend that every security organization assess the changes in their threat and vulnerability landscapes over the past two years and adjust their cyber security controls as needed to address new or growing areas of risk," Schaufenbuel says.

7. Communication is vital for effective IR in a remote environment and must be addressed differently in a hybrid work environment as opposed to one with employees in central offices.

"If you aren't sure who is where on what day, you need to look at how that affects alerts and ongoing communication with members of the IR team and for all employees," Burn says.

8. Automation and education are key to securing organizations in the hybrid/remote work environments.

"The escalating threat landscape is driving higher incident volumes," Schaufenbuel says "Because incident response teams are not growing as fast as incident volumes, incident response teams must automate responses. Investments in security orchestration and automated response technology are becoming more important than ever."

9. Whenever possible, automate incident detection, response, and mitigation.

In many cases companies are asking for that capability, Tolman says. The greater need for automation "is kind of the consequence of the [skills] shortage," he says.

10. Train employees to recognize and report suspicious activity.

So is the greater need for training and education programs. "You need to educate your workforce," Tolman says. That includes teaching remote workers about best practices for operating devices and networks, and how to look out for suspicious activities and avoid falling prey to malware and phishing attacks.

Solid training programs can help organizations build more proactive cyber security approaches, by trying to keep a step ahead of the bad actors.

"Since end users working from home are being targeted more by attackers, and the best response to an incident is to avoid it to begin with, additional investments in security awareness training can have a huge positive impact," Schaufenbuel says.

Conclusion

There is no turning back. The pandemic forever changed the workforce models in place at many organizations worldwide. Today, hybrid and remote work arrangements are the norm, and IT and security executives need to embrace the concept and do their best to support the new models.

At the same time, security threats have only become more pervasive and insidious. Data breaches, ransomware attacks, malware, and other security threats are a constant concern. The shift to remote work has increased the level of risk because more than ever the corporate firewall can no longer be relied upon as a bastion of defense.

Organizations need to be able to detect and respond to incidents regardless of where users are working or which types of devices they are using.

By taking the steps described above, including deploying tools designed to support incident response remotely, enterprises can bolster their security in this new environment.