Mighty Guides

Sponsored by Trustwave®

7 Experts on Transforming Your Threat Detection & Response Strategy

Protection for the ongoing evolution of your workforce

INTRODUCTION

In light of COVID-19 and other recent events, our world has grown increasingly connected but also more complex and vulnerable. Security professionals must create a threat-detection and response strategy that is resilient while addressing the rapid digital transformation organizations need to continue functioning. How can security leaders rise to this challenge in 2020 and beyond?

With generous support from Trustwave, we asked seven security experts for their advice for transforming your threat-detection and response strategy.

Many security leaders emphasize the importance of following a strong yet flexible security framework. Others recommend testing your security plan, particularly if your organization has a global footprint. Depending on your situation and industry, establishing a strong partnership with a managed security service provider (MSSP) or managed detection and response (MDR) provider can help you achieve your security goals.

The essays in this eBook offer practical strategies, advice, and examples from seasoned professionals that will help you transform your threat-detection and response strategy. They explain how to identify obvious and less obvious gaps in your strategy, create and implement a flexible threat-detection and response strategy, and much more. If you have been charged with defending your organization against evolving threats, you will benefit from the wisdom these experienced security professionals have shared.

All the Best,
David Rogelberg
Publisher, Mighty Guides, Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

FOREWORD

This book would not have been possible without the combined efforts of several individuals at both Trustwave and Mighty Guides. Suffice it to say, the year 2020 has been unprecedented to anything experienced by current generations. The obstacles faced over the last several months have challenged organizations to rethink their operational models and approaches in almost every sense, including in terms of security, human relations, and safety. Rapid adaptations that were necessary to maintain business continuity introduced new risks that were immediately taken advantage of by unscrupulous actors. 'Steady state' is no longer sufficient. If your organization is not continuously changing to meet the rapidly evolving demands of an aggressive and dynamic threat landscape, you may be left behind.

A culmination of original ideas, research, and new field findings, 7 Experts on Transforming Your Threat Detection & Response Strategy emphasizes the importance of a proactive security approach in the modern age. No longer can security operations be simply reactive, because just as technology is continuously evolving, hackers, adversaries, and threats are quickly evolving to exploit weaknesses and uncertainty. We encourage you to transform your approach to ensure efficient detection and eradication of threats and to achieve resilience to the challenges thrown your way.

Regards,
Jesse Emerson,
Vice President, Managed Threat Detection and Response (Americas)

Trustwave®

Trustwave is a leading cybersecurity and managed security services provider focused on threat detection and response. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries. For more information about Trustwave, visit:

www.trustwave.com

TABLE OF CONTENTS

MEET OUR EXPERTS

DAVID VAN
VP InfoSec Engineering and Operations,
Investors Bank

DENEEN DEFIORE
Vice President & Chief Information Security Officer,
United Airlines

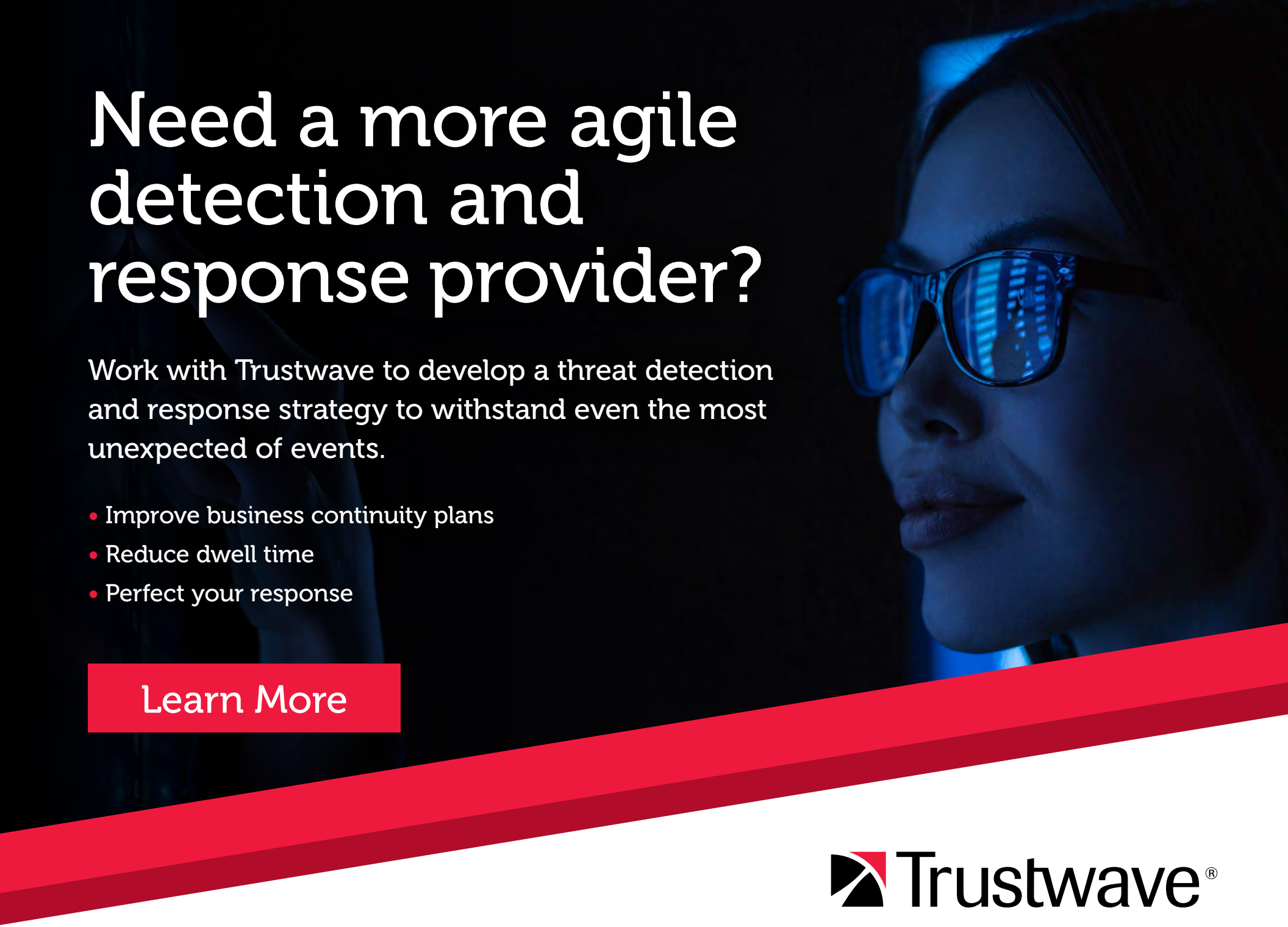
DMITRIY SOKOLOVSKIY
Chief Information Security Officer
Avid Technology

FELIPE MEDINA
VP of Information Security Architecture and Operations,
BankUnited

GENADY VISHNEVETSKY
Chief Information Security Officer,
Stewart Title

MATTHEW OTWELL
Chief Information Security Officer,
MD Department of Health

NIKK GILBERT
CISO,
Confidental


Need a more agile detection and response provider?
Work with Trustwave to develop a threat detection and response strategy to withstand even the most unexpected of events.
• Improve business continuity plans
• Reduce dwell time
• Perfect your response
Learn More
Trustwave®

CHAPTER 1

IDENTIFY GAPS AND RISKS IN YOUR SECURITY OPERATIONS

Security professionals know that it is critical to proactively and consistently identify any gaps or risks that exist in security operations, continually testing assumptions along the way. In light of the landscape changes brought on by the recent pandemic, this work could not be more urgent or important for how and where we work in the future. We looked at how organizations tackle this frequent challenge and asked our experts the following questions:

- ***How has the day-to-day effectiveness of your security operations team been challenged?***
- ***What additional capabilities do you need to make your organization more resilient?***
- ***What advice can you offer security leaders for identifying obvious and less obvious gaps?***

David Van, Investors Bank, VP InfoSec Engineering and Operations

An information security professional with a demonstrated history of working in the banking industry. Skilled in IT infrastructure management, cloud security, information security, IT Infrastructure operations, and virtualization. Strong operations professional with a Bachelor of Arts in Mathematics and Computer Science from Binghamton University. Security certifications include CISSP and CCSP.

"Before the pandemic, we used intrusion detection sensors to identify abnormal behavior on the network."

Before the pandemic, we used intrusion detection sensors to identify abnormal behavior on the network. We put in network access control products to detect an unauthorized foreign object trying to get onto a network. We had been deploying different security controls and tools for decades, assuming that the bulk of the employees were working from a corporate office and using a private network.

When everybody began working from home, none of those sensors was effective anymore. Overnight, our security controls had to shift to the individual endpoint — basically, the users' computing devices. We originally had an infrastructure topology protection of the data centers, the servers, and the network, with everything on premises. The next morning, we needed to make sure that we were protecting Joe, Sam, and Lily — all the employees of every department.

You need three capabilities, or three Cs, to be resilient in this kind of situation: connectivity, communications, and collaboration. If one of these three things stops working, remote operations will fail. If you have a problem connecting, you cannot do business. If you cannot

communicate among teams, you cannot conduct business. If you cannot collaborate, you cannot do business. No business exists in a vacuum, right? These three critical capabilities must become resilient immediately.

“When everybody began working from home, none of those sensors was effective anymore.”

Deneen DeFiore, Vice President & Chief Information Security Officer, United Airlines

Deneen DeFiore is VP and CISO for United Airlines. She is responsible for shaping United's cybersecurity strategy to ensure that the company is prepared to respond to evolving cyberthreats and regulatory obligations. She also leads the company's initiatives on commercial aviation cybersafety risk and improving cyber resilience. She works with industry partners to reduce cybersafety risk worldwide across the aviation ecosystem.

"The pandemic has dramatically changed our threat model and attack surface."

The pandemic has dramatically changed our threat model and attack surface. We had to reevaluate our threat intelligence collection priorities, look again at our tuning or our security technology and solutions, and verify that we didn't have gaps or blind spots resulting from changes in the network to enable everybody to work from home. A few challenges appeared at first involving the effectiveness of the team as it adjusted to completely virtual operating cadences. Some of the response techniques or forensics toolings and processing processes relied heavily on our being on our network or in a building versus being completely remote, and that was a challenge that we had to overcome as well.

Resourcing was also an issue. There was definitely a surge in work to respond to the crisis in terms of risk mitigation and planning. We had to make sure that we had coverage if people were out or ill, or when third parties that we rely on had issues. We noticed a significant surge in phishing and social engineering threat activity that I think everybody was encountering at the time. We had to respond to that and make sure we were keeping our company safe. The result was a lot of work and a lot of long hours for everyone. ■

“Many companies have pandemic plans, but until they actually experience a pandemic, they don’t know how far from reality that plan actually is.”

When COVID-19 hit, we thought we were all set. Reality hit us slightly earlier than the majority of the world because we had an office presence in Manila, Philippines, and right before the pandemic, a volcano there came close to erupting. We were already going through disaster recovery and business continuity preparation because of that potential office impact. Then, COVID-19 started spreading. We realized that the preparations we had made for the volcano were not sufficient. Many companies have pandemic plans, but until they actually experience a pandemic, they don’t know how far that plan actually is from reality.

We learned that our preparation must involve local representation. You should be talking to and learning about your local teams’ day-to-day difficulties because in some cases, you may not have accounted for simple logistics in your planning. In some locations, for example, your people won’t be able to bring a desktop computer home; even if they were able to, there may be no reliable internet connection at home. That was an eye-opening experience for us. We were about a month ahead of the curve, so we were able to address connectivity, and COVID-19 didn’t affect us the way it could have if we were not already preparing for a disaster. ■

Dmitriy Sokolovskiy, Chief Information Security Officer, Avid Technology

Since 1999, Dmitriy has consulted defense contractors, financial and medical companies, and nonprofits. In 2007, he created CyberArk’s Implementation Services teams, and personally participated in the largest breach remediation events. In 2016, Dmitriy was the SaaS product Cloud Security Architect, and in 2018, Dmitriy became the CISO for Avid Technology, where he advises information security start-ups, and venture capital firms. Dmitriy is also a member of the GIAC Advisory Board and holds the GISF, GCED and CISSP certifications.

Felipe Medina, VP of Information Security Architecture and Operations, BankUnited

Felipe Medina is responsible for establishing and maintaining a corporate-wide information security technology program to ensure that information assets are adequately protected both on premises and within multiple cloud environments/ technologies. This includes having an up-to-date understanding of the latest security threats, trends, and technologies, managing and supporting existing security solutions, evaluating, designing, and implementing new technical security controls, and working to meet security objectives.

"Make sure that you have good disaster recovery and business continuity plans and that you test them at least once or twice a year."

Make sure that you have good disaster recovery and business continuity plans and that you test them at least once or twice a year. Even before I arrived at BankUnited, we had a mature solution for testing in place. We performed yearly tests right before hurricane season because we are based in the Miami, Florida, area. COVID-19 just accelerated that planning to a 100 percent remote situation.

Because of our thoroughness in testing and the road map that we had set forth as a company, we were able to transform ourselves quickly. I think that it's a matter of not just having a business continuity plan but also testing that plan thoroughly every year so that everyone knows what his or her roles and responsibilities are.

When we run these tests, we work hand in hand with our internal audit department and our IT risk teams to make sure that we have everything covered. On top of that, we conduct external penetration tests quarterly rather than once a year — something most other organizations don't do. We receive constant feedback on the program, our security visibility, and our posture so that we can make frequent improvements. This year, we will also become more of an internal purple team, testing all our controls and security processes as well.

“We must prepare for a scenario in which our users (or some subset of them) will never come back to the office.”

It is safe to assume that your workers will never come back to the office. I know it sounds extreme, but companies such as Facebook, Amazon, and Google have already announced that employees who can be productive working remotely are allowed to do so, some indefinitely. We must prepare for a scenario in which our users (or some subset of them) will never come back to the office. The questions you must ask include: How will you restructure your security program? Should you support bring your own device, and, if so, should you limit to corporate-issued devices? Should you shift to a virtual desktop infrastructure so that you don’t have to worry about users’ devices?

Focus on the endpoint and the edge. The edge can be anywhere now, so you must be prepared to implement compensating controls for both the managed and unmanaged edge. The managed edge could be a software-defined wide-area network — that is, a connection for satellite offices — if users return to the office. A home Internet connection would be an example of unmanaged edge. Home Wi-Fi brings up another challenge: How do you secure something you don’t control or even have access to? Many of us do not have the luxury to conduct a deep network analysis on the firewalls, so we must completely shift our detection strategy to the endpoint. ■

Genady Vishnevetsky, Chief Information Security Officer, Stewart Title

Genady Vishnevetsky serves as the Chief Information Security Officer (CISO) for Stewart Information Services Corporation, a leading provider of real estate services, including global residential and commercial title insurance, escrow and settlement services, lender services, underwriting, specialty insurance, and other solutions that facilitate successful real estate transactions. An established leader with experience in building a successful security program and developing the defense against emerging threats, Vishnevetsky leads the security, governance and compliance program for the global enterprise.

Matthew Otwell, Chief Information Security Officer, MD Department of Health

Matthew Otwell has been an IT and Information Security professional working with multiple global or state organizations over a 25-year span. Currently, Mr. Otwell serves as the CISO for the MD Department of Health. His educational background includes a Bachelor of Science in Electronics Engineering Technology from Capitol University and multiple certifications including CISM (Certified Information Security Manager), CCSK (Certificate of Cloud Security Knowledge), and ITIL v.3 Foundation.

"When you've identified the gaps and put your plans in place, the next challenge is effectively communicating how you're going to handle and remediate the gaps you've identified."

The COVID-19 pandemic is not selective; it can affect every person. For any organization, the health and safety of its personnel should be the primary focus. From there, you can begin to visualize what the post-pandemic work environment will be for your organization. Following a good security framework and model will help you with this visualization, enabling your security leaders to identify some of the obvious and less obvious gaps.

From an information security perspective, identifying gaps is particularly challenging, especially because most organizations are reactive rather than proactive. One way to identify gaps is to implement a scorecard. That way, while following a good security framework and security model, you can identify where deficiencies exist.

When you've identified the gaps and put your plans in place, the next challenge is effectively communicating how you're going to handle and remediate the gaps you've identified. You can have the best plan in the world, but if you can't effectively distribute and communicate it, the plan will be ineffective. Understand the proper channels of communication within your organization so that you can disseminate important information in a timely manner.

“Ultimately, however, you put all the technical stuff aside because it’s about the people. It’s about making sure that your people are taken care of.”

What really surprised me was that people are much more resilient than I ever imagined. As things progressed with the pandemic, we made the business decision to move to a remote workforce. My team members embraced the transition. They are more effective now than they have ever been. They have more time; fewer “drive-bys,” if you will; and fewer distractions than they did in the traditional office setting.

As the signs of this pandemic became more apparent and we started considering working from home, we looked at our infrastructure and said, “What do we need to improve to increase or streamline the service?” One thing we found was that our virtual private network (VPN) connectivity was not as robust as we needed it to be. Fortunately for us, we had access to the right technology. We were able to meet the requirements when the time came by being proactive, understanding what our limitations were, and making adjustments.

When something like the COVID-19 pandemic hits, you’ve got to look at your environment and organization holistically, figure out how you can continue to operate. You have to adjust accordingly. Ultimately, however, you put all the technical stuff aside because it’s about the people. It’s about making sure that your people are taken care of. ■

Nikk Gilbert, CISO, Confidental

With 20 years of executive level experience in information technology roles, Nikk is a respected thought leader within the government & private sectors. Nikk holds the CISSP and CISM security certifications and has been a keynote speaker at technology events throughout the world.

CHAPTER 2

EVALUATE YOUR INCIDENT RESPONSE PLAN

In addition to regularly identifying gaps and risks in your security operations, you must review your incident response plan so that your organization is in the strongest possible position to respond in the event of an attack. Many security leaders, having noticed areas for improvement in their incident response in the wake of the pandemic, have begun strengthening their own incident response capabilities. We explored how they do this by asking them the following questions:

How have you altered your incident response plan to limit the impact of a security incident?

How are you working with your current MSSP or MDR provider to improve this plan?

What kind of guidance can you give security leaders who are considering a partnership with an MSSP or MDR provider to improve their incident response capabilities?

David Van, Investors Bank, VP InfoSec Engineering and Operations

An information security professional with a demonstrated history of working in the banking industry. Skilled in IT infrastructure management, cloud security, information security, IT Infrastructure operations, and virtualization. Strong operations professional with a Bachelor of Arts in Mathematics and Computer Science from Binghamton University. Security certifications include CISSP and CCSP.

“You must completely change your CIRP to reflect the fact that your endpoints are your vulnerabilities and your infrastructure is not the primary target anymore.“

A cyber incident response plan (CIRP) focuses on traditional security topologies, which consist of network security, perimeter security, and server storage security. These are the typical points where detection happens. An event occurs, it’s analyzed and verified, a trigger occurs, and that event becomes an incident. A CIRP immediately calls on all the right stakeholders and resources. Those people come to the office and start shutting down the network to contain the violation or compromised resource.

Today, you have thousands of endpoints, and any one of them could be compromised. The focus is on how you respond to an event or incident that happens on someone’s computer in Jersey City as opposed to a corporate office or data center. You must completely change your CIRP to reflect the fact that your endpoints are your vulnerabilities and your infrastructure is not the primary target anymore.

One of the driving forces of MDR is that the world is transitioning from on-premises infrastructures to cloud infrastructures. The pandemic has made MDR even more significant. Not only are people already accessing resources in the cloud with little dependency on a virtual private network

or the corporate network, but the pandemic is also driving the majority of users to go out to the cloud directly. That's why MDR is what's needed in today's environment.

"The pandemic has made MDR even more significant."

Deneen DeFiore, Vice President & Chief Information Security Officer, United Airlines

Deneen DeFiore is VP and CISO for United Airlines. She is responsible for shaping United's cybersecurity strategy to ensure that the company is prepared to respond to evolving cyberthreats and regulatory obligations. She also leads the company's initiatives on commercial aviation cybersafety risk and improving cyber resilience. She works with industry partners to reduce cybersafety risk worldwide across the aviation ecosystem.

"Communication and partnership with your providers have to be more collaborative and inclusive."

We treat our MSSP as an extension of our team and our security operations capability. It's about ensuring that the MSSP team members understand the priorities, know the threat landscape, are clear about what they should be looking for, and embrace our expectations for a response. All this is especially important now because things have changed so rapidly. Communication is vital, so make sure that you disseminate the changes you're making quickly. A bit of negotiation may be required, as well. New requirements that would have been negotiated over a couple of weeks before the pandemic — well, that timeline is probably no longer acceptable. Things need to be done in a day or two now.

When some companies began to allow their employees to work from home, they may have had a couple of virtual private network (VPN) connections. Now, in the new landscape, it's all VPN connections. That means integrating those log sources having the right threat models, indicators of compromise, and alerts firing; and defining the right thresholds for when escalations are necessary. Such tasks will have to be done in a snap now, whereas before they would have been a project. Timelines are accelerated now. Communication and partnership with your providers have to be more collaborative and inclusive. ■

“We conduct a monthly exercise using role-playing runs, and we learn something after each one.”

Dmitriy Sokolovskiy, Chief Information Security Officer, Avid Technology

Practice your incident response plan. A security vendor released a card game, similar to Cards Against Humanity, called Backdoors and Breaches. Basically, it’s a card game about information security incidents. In the beginning of the game, you have the manager — me, for example — running the incident and distributing the cards to my team. The cards are about some form of what’s going on, and then actions that the team can take. You present the team with a situation, and the team members have to go through it.

The team should have a plan, and it should follow through with that plan. You make some assumptions in the game, too. You roll a die to add randomness to the situation. A role-playing game puts you through the steps at no risk. That’s the best time to learn that you don’t know how to do something or haven’t accounted for something in your plan.

The plan you use as a model doesn’t have to be detailed, but you’ve got to start it, and you’ve got to build on it. We conduct a monthly exercise using role-playing runs, and we learn something after each one. In some cases, we may adjust the plan. That’s part of our ongoing preparation for incidents. ■

Since 1999, Dmitriy has consulted defense contractors, financial and medical companies, and nonprofits. In 2007, he created CyberArk’s Implementation Services teams, and personally participated in the largest breach remediation events. In 2016, Dmitriy was the SaaS product Cloud Security Architect, and in 2018, Dmitriy became the CISO for Avid Technology, where he advises information security start-ups, and venture capital firms. Dmitriy is also a member of the GIAC Advisory Board and holds the GISF, GCED and CISSP certifications.

Felipe Medina, VP of Information Security Architecture and Operations, BankUnited

Felipe Medina is responsible for establishing and maintaining a corporate-wide information security technology program to ensure that information assets are adequately protected both on premises and within multiple cloud environments/ technologies. This includes having an up-to-date understanding of the latest security threats, trends, and technologies, managing and supporting existing security solutions, evaluating, designing, and implementing new technical security controls, and working to meet security objectives.

"We have a SNOC management team, and several third parties helped us build playbooks and run books before COVID-19 changed the way we work."

Our incident response plan really hasn't taken a hit because of COVID-19. We had already begun introducing the new platforms that perform our endpoint detection and response (EDR) functionality, so we were set on that front. Right before the pandemic, however, we onboarded a security and network operation center (SNOC) — a 24/7 monitoring service that we set up. We have a SNOC management team, and several third parties helped us build playbooks and run books before COVID-19 changed the way we work.

Everything in security is a matter of planning and budgeting, so it took a while to get up and running. The SNOC took about two years to complete — from its ideation phase to its inception. It went live in February. Then, in March, what was happening with the pandemic became clear. Shortly after April, we started allowing people to work remotely. We've had to tweak that incident response plan very little because we were already building up our platforms to prevent a hit.

“The ability to quickly quarantine a process, a program, or an entire device will become vital to incident response.”

The endpoint has become the primary focal point for incident detection and response. The ability to quickly quarantine a process, a program, or an entire device is fundamental in responding to the incident. When a user reports a malicious URL or abnormal behavior on the endpoint is detected, you must be able to disseminate this information across your enterprise rapidly and make sure that all your other users are blocked from accessing the URL — a vital step when the majority of threats come through phishing emails.

Email security gateways are getting better every day, but they’re still flawed. Security leaders must be able to block and retract emails quickly if they’re found it to be malicious, even after having passed security technologies.

Endpoint detection and response (EDR) and MDR will become primary detection and remediation mechanisms. All vendors will have to offer them, whether they buy them or develop their own. That’s my crystal ball.

All the traffic and much of the communication that came from traditional office spaces will probably become extinct in the near future, so the key is to start evaluating behaviors, not locations. I could be in South America or Europe. Evaluate my behavior. Does it meet the criteria of normal me?

Genady Vishnevetsky, Chief Information Security Officer, Stewart Title

Genady Vishnevetsky serves as the Chief Information Security Officer (CISO) for Stewart Information Services Corporation, a leading provider of real estate services, including global residential and commercial title insurance, escrow and settlement services, lender services, underwriting, specialty insurance, and other solutions that facilitate successful real estate transactions. An established leader with experience in building a successful security program and developing the defense against emerging threats, Vishnevetsky leads the security, governance and compliance program for the global enterprise.

Matthew Otwell, Chief Information Security Officer, MD Department of Health

Matthew Otwell has been an IT and Information Security professional working with multiple global or state organizations over a 25-year span. Currently, Mr. Otwell serves as the CISO for the MD Department of Health. His educational background includes a Bachelor of Science in Electronics Engineering Technology from Capitol University and multiple certifications including CISM (Certified Information Security Manager), CCSK (Certificate of Cloud Security Knowledge), and ITIL v.3 Foundation.

"In the wake of COVID-19, we have realized that the most important action we need to take in regard to incident response is to improve our documentation and communication."

The Maryland Department of Health does not currently have an MSSP in place for incident response; we do it all in house. In the wake of COVID-19, we have realized that the most important action we need to take in regard to incident response is to improve our documentation and communication. Many employees within our organization know what to do when an incident occurs, but knowing the difference between disaster recovery and business continuity is another matter.

If those specific individuals who are responding to an incident are not available because of a crisis, we have to ask ourselves, "Who would do the work, and what would they do?" So, we're not really changing our incident response plan per se. The process is still the same, but we're making sure that we're documenting and communicating so that we can invoke the plan, if necessary, during a future crisis.

When this documentation is complete, security leaders can evaluate the plan and decide how to execute it. Then, they can determine, from both a cost and a business risk perspective, whether they have the appropriate resources to execute the plan or should engage an MSSP. Engaging an MSSP has certain advantages. For example, you can stipulate service level agreements within your contractual agreements that could greatly improve your incident response effectiveness.

“Your incident response plan is one of the most important documents you have.”

Your incident response plan is one of the most important documents you have. You’ve got all your security protections in place. You’ve done all your security training. You’ve trained your users, you’ve got your technology, you’ve got your defense in depth. You’ve got all these different pieces of the puzzle and technological wonders to protect against all the bad actors out there trying to steal money or data. At the end of the day, however, how you respond to what happens determines whether you still have your job.

So, you need a strong, formalized incident response plan that is recognized at the highest levels of the organization. Leadership must approve the plan to show that they understand its value and importance to the organization. Look at companies that had a strong incident response plan. One that I love to bring up is Nationwide Insurance. Nationwide had a breach a couple of years ago, and it nearly went unnoticed in the media. The company’s strong incident response plan was well practiced and had buy-in at the highest levels of the organization. A third-party partner that helps you develop your incident response plan can put you in a position to respond correctly when an incident happens.

Nikk Gilbert, CISO, Confidental

With 20 years of executive level experience in information technology roles, Nikk is a respected thought leader within the government & private sectors. Nikk holds the CISSP and CISM security certifications and has been a keynote speaker at technology events throughout the world.

CHAPTER 3

EXPAND YOUR VISIBILITY

The threat landscape was already changing as a result of many organizations beginning to support the needs of a remote workforce and transitioning to the cloud, so the pandemic accelerated an already-rapid digital transformation. This acceleration has highlighted the importance of not only maintaining but expanding your visibility across your threat landscape, passing far beyond the traditional perimeter to encompass end points and cloud infrastructure, among other elements. We looked at how companies achieve the visibility they seek by asking security leaders the following questions:

What steps have you taken to ensure that your security operations team has visibility into the new operating environment?

What steps are you taking to develop and maintain your security monitoring use cases?

What advice can you offer for expanding the scope of threat detection and response in the new landscape?

David Van, Investors Bank, VP InfoSec Engineering and Operations

An information security professional with a demonstrated history of working in the banking industry. Skilled in IT infrastructure management, cloud security, information security, IT Infrastructure operations, and virtualization. Strong operations professional with a Bachelor of Arts in Mathematics and Computer Science from Binghamton University. Security certifications include CISSP and CCSP.

"First, you must understand the three kinds of visibility you need into your environment."

First, you must understand the three kinds of visibility you need into your environment. You must be able to spot anomalies — user behaviors that don't match your baseline for expected patterns of usage. Then, you need visibility that's powered by straightforward automation — simple rules for granting and denying access based on common scenarios. For example, if David tried to authenticate five times and failed, technology will prevent him from getting in. A human element is also necessary; however, the ability to make informed, contextual judgment calls about granting or revoking access is based on standard operating procedures (SOPs). MDR agents can handle these three types of visibility at the human level.

Once you understand the three kinds of visibility, you can create a road map to match. If you're weak on the artificial intelligence (AI) portion, for example, you may want to explore an MDR solution that can help you detect anomalies. If you don't have a process for a human to inspect access based on context, looking beyond the simple yes/no question of whether someone should have access, evaluating the granular level of access that user should have, and determining how often the user should have it, you may want to create manual SOPs to handle that kind

of visibility. There are many ways to get started, but these are generally the three elements a company needs to reach maturity from a visibility perspective.

“If you’re weak on the AI portion, for example, you may want to explore an MDR solution that can help you detect anomalies.”

Deneen DeFiore, Vice President & Chief Information Security Officer, United Airlines

Deneen DeFiore is VP and CISO for United Airlines. She is responsible for shaping United's cybersecurity strategy to ensure that the company is prepared to respond to evolving cyberthreats and regulatory obligations. She also leads the company's initiatives on commercial aviation cybersafety risk and improving cyber resilience. She works with industry partners to reduce cybersafety risk worldwide across the aviation ecosystem.

"You will have to augment your cloud capability to gain visibility."

If your business is accelerating its digital transformation strategy to move its workloads to the cloud, then you have to adapt your security approach to support that strategy. Make sure that you have a strong integration into the strategy and that you're setting up the security architecture not just from an application security perspective but also from an instrumentation, monitoring, logging, and detection perspective.

Many cloud platforms have great native tools that you can use as you're getting started, but they won't be the end all, be all. You will have to augment your cloud capability to gain visibility. We start with the native capabilities, and then add commercial tooling. It's also worth looking at cloud compliance and policy monitoring. That kind of continuous monitoring is really what helps us. You don't always want to be in detection mode, right? You want to make sure that if you're in the cloud, you're taking advantage of being in the cloud. Orchestration and automation can find things, self-heal, and remediate issues quickly.

“Similar to running tabletop exercises for incident response, run a tabletop brainstorming session about the logs once a quarter or maybe twice a year.”

Detection is always a battle of false positives versus false negatives. If your detection mechanisms are too tight, you get too much noise. In my opinion, that’s more counterproductive than missing a real alert. Figuring out how tight you make your alerts is a challenge because most of today’s tools will generate an alert for almost everything except for rare zero days or maybe advanced adversaries.

Most of the time, you’re going to find what you’re looking for. The problem is finding it in the haystack of other things. You can use logs of all kinds for forensics and research. Similar to running tabletop exercises for incident response, run a tabletop brainstorming session about the logs once a quarter or maybe twice a year.

Assemble people in a room or, because we’re not in a room these days, on a video conference. Begin by saying, “These are the things we’re collecting.” The goal is for people simply to ask, “Hey, what about this? What about that?” You’re trying to discover whether there’s something you know you can collect but you’re not because you simply didn’t think of it. Make sure that the coverage is as wide as it can be. ■

Dmitriy Sokolovskiy, Chief Information Security Officer, Avid Technology

Since 1999, Dmitriy has consulted defense contractors, financial and medical companies, and nonprofits. In 2007, he created CyberArk’s Implementation Services teams, and personally participated in the largest breach remediation events. In 2016, Dmitriy was the SaaS product Cloud Security Architect, and in 2018, Dmitriy became the CISO for Avid Technology, where he advises information security start-ups, and venture capital firms. Dmitriy is also a member of the GIAC Advisory Board and holds the GISF, GCED and CISSP certifications.

Felipe Medina, VP of Information Security Architecture and Operations, BankUnited

Felipe Medina is responsible for establishing and maintaining a corporate-wide information security technology program to ensure that information assets are adequately protected both on premises and within multiple cloud environments/ technologies. This includes having an up-to-date understanding of the latest security threats, trends, and technologies, managing and supporting existing security solutions, evaluating, designing, and implementing new technical security controls, and working to meet security objectives.

"As with any monitoring, expanding your visibility requires constantly creating new baselines."

As with any monitoring, expanding your visibility requires constantly creating new baselines. The first step is filtering out the noise. The next step is building the proper use cases for what you want to monitor in phase 1 and developing more advanced use cases as you proceed. Continuity between the teams is important. The SNOC team knows exactly what we want to enhance, and they know what our road map is. Similarly, upper management has bought into what we're doing and why we're doing it. We keep the lines of communication open.

Every plan and platform requires feedback from multiple teams. When we went with our new antimalware and EDR platform, more people than just my team were involved. We brought in the cybersecurity team, the SNOC, our cloud architecture team, and our infrastructure and operations team. We brought in our wide-area network team to show the differences between the legacy platform and the new one, and then we all voted. When the vote is unanimous, it's great. When there's contention, however, we hit the pause button and say, "What do we need to go ahead? What did we miss that you're concerned about so that we can better scope for any future platform we consider?"

“The edge is getting closer to the endpoint, so chief information security officers need visibility into their endpoints.”

The edge is getting closer to the endpoint, so chief information security officers (CISOs) need visibility into their endpoints. We have found that most of the tools we rely on have some kind of console to manage endpoints. Make sure your monitoring tools are accessible from outside of your office. Create a baseline of user common locations and normal behavior so you have a starting point to full user visibility. Make sure you have endpoint protection (EPP), EDR, or MDR agents as well as a data loss prevention (DLP), and web proxy installed. User behavior is a key consideration. Consider adding end-user behavior analytics tools, if you don’t have them already, to your security operations center.

Everything is going to the cloud, and so visibility is key. Cloud security has become incredibly important. Cloud access security brokers (CASB) are worth considering. Make sure that you can rapidly deploy everything in the cloud or outside of your office — anything from configuration changes to deploying updates or new agents and tools.

Finally, consolidate data governance. For example, for Microsoft 365 users, a full ecosystem is extremely beneficial: email and its protection, OneDrive for Business, OneNote, SharePoint for data storage and intranet, DLP, and endpoint protection. That way, you have a 360-degree view into your environment, with full visibility into and control of your data storage and flow.

Genady Vishnevetsky, Chief Information Security Officer, Stewart Title

Genady Vishnevetsky serves as the Chief Information Security Officer (CISO) for Stewart Information Services Corporation, a leading provider of real estate services, including global residential and commercial title insurance, escrow and settlement services, lender services, underwriting, specialty insurance, and other solutions that facilitate successful real estate transactions. An established leader with experience in building a successful security program and developing the defense against emerging threats, Vishnevetsky leads the security, governance and compliance program for the global enterprise.

Matthew Otwell, Chief Information Security Officer, MD Department of Health

Matthew Otwell has been an IT and Information Security professional working with multiple global or state organizations over a 25-year span. Currently, Mr. Otwell serves as the CISO for the MD Department of Health. His educational background includes a Bachelor of Science in Electronics Engineering Technology from Capitol University and multiple certifications including CISM (Certified Information Security Manager), CCSK (Certificate of Cloud Security Knowledge), and ITIL v.3 Foundation.

"A good information security framework can expand or contract based on the threat landscape."

As we face the rapid digital transformation accelerated by COVID-19, we are reevaluating the threat landscape. We had to think outside the box to determine the extent of that new threat landscape. When we had developed a picture of what this new environment looked like, specifically for an extended remote workforce, and we were able to identify the controls required to reduce the new risks and exposures introduced in the expanded threat landscape. I always go back to having a solid information security framework in place: A good information security framework can expand or contract based on the threat landscape.

The technical security controls you have implemented can give you greater visibility into your environment. Make sure that you have enough licenses to support all your devices, including the desktop and laptop computers that users will connect from remote locations. Make sure that you have a good asset-management system to address and verify any additional security concerns that come up with the expanded remote workforce. My strongest recommendation is to make sure that you're thinking about what that expanded landscape may look like. Confirm that you have everything in place from a licensing perspective, from a connectivity perspective, and from an asset-management perspective. That way, you can address the visibility challenges of a remote workforce environment. ■

“Look at all the changes you have had to make since the pandemic started.”

Look at all the changes you have had to make since the pandemic started. As you do, make sure that you’ve got processes and procedures in place to protect yourself from any bad outcomes that may result from those new scenarios. A great example is the bad actors who are trying to hack VPN connectivity. Make sure that you are using enterprise-licensed tools that provide the right level of protection. Organizations that have been using tools such as Zoom have experienced major vulnerabilities.

If you are lucky enough to have an enterprise-level tool that is secure, then you don’t have to worry. If you don’t have such a tool, look at everything you have done, every tool you have changed or added to your toolbox since the pandemic started, and evaluate it. In addition, constantly monitor your environment to make sure that you are not missing something. Otherwise, bad actors may be able to attack your organization and steal your users’ information. Similarly, document any changes you make so that you can review them and make sure that you’ve got processes, procedures, and controls in place to address any issues.

Nikk Gilbert, CISO, Confidental

With 20 years of executive level experience in information technology roles, Nikk is a respected thought leader within the government & private sectors. Nikk holds the CISSP and CISM security certifications and has been a keynote speaker at technology events throughout the world.

CHAPTER 4

CREATE A FLEXIBLE THREAT-DETECTION AND RESPONSE STRATEGY

As the pandemic showed us, a flexible threat-detection and response strategy is fundamental to successfully navigating an unexpected crisis with agility and precision, but how can organizations create such a strategy while balancing organizational goals and budget constraints? To shed some light on the subject, we asked security experts the following questions:

What should a security leader consider when creating a more flexible threat-detection and response strategy that will be resilient in the face of rapid change?

How are you prioritizing your organizational goals and budgets to define how you move forward?

What advice can you offer security leaders for prioritizing improvements?

David Van, Investors Bank, VP InfoSec Engineering and Operations

An information security professional with a demonstrated history of working in the banking industry. Skilled in IT infrastructure management, cloud security, information security, IT Infrastructure operations, and virtualization. Strong operations professional with a Bachelor of Arts in Mathematics and Computer Science from Binghamton University. Security certifications include CISSP and CCSP.

"The goal is to have an MDR because the MDR is going to give you the three kinds of visibility you need."

The word create means different things to different people. When you create something, are you coming up with a plan, or are you actually developing an implementation? In this case, the creative part should involve developing a plan that takes you from wherever you are today to the MDR era. The goal is to have an MDR because the MDR is going to give you the three kinds of visibility you need. The MDR offers three types of detection: anomalies detected by AI, automation to detect yes/no conditions, and the special procedures to have someone in the business identify whether to grant access to specific resources in the context of the business need.

To achieve that goal, you need two things. First, you need an MDR partner that has the ability to give you what you need. Some MDR providers are more appropriate for beginners, while others may have a lot of fancy bells that you don't need. Second, the MDR provider should have expertise in your industry. If you talk to an MDR provider that is good with pharmaceuticals but you are in the oil industry, that provider won't know much about your regulations and won't understand the privacy applications required for your particular customer base. I recommend that enterprise security leaders take all these pieces into consideration as part of their strategy and planning.

Deneen DeFiore, Vice President & Chief Information Security Officer, United Airlines

Deneen DeFiore is VP and CISO for United Airlines. She is responsible for shaping United's cybersecurity strategy to ensure that the company is prepared to respond to evolving cyberthreats and regulatory obligations. She also leads the company's initiatives on commercial aviation cybersafety risk and improving cyber resilience. She works with industry partners to reduce cybersafety risk worldwide across the aviation ecosystem.

"You have to be able to understand what is critical to your business."

A critical point to consider is how to use your threat landscape and organizational risk to inform what your detection, processes, and strategy are going to be. If you just look at your threat-detection and response strategy without those lenses, it could be overwhelming. You have to be able to understand what is critical to your business. Using that quality intelligence to inform your response is crucial. It is not a one and done thing, either: You must review your strategy continuously, inform your programming, and evolve.

That approach will enable you to be resilient and respond as risks change and threats manifest differently. Another good practice and sound strategy is to make sure that you have incident response playbooks for the different types of events you expect to face. Define and continuously improve and enhance these playbooks as intelligence informs them, because tactics, techniques, and procedures are going to change, as well. You can't be locked in and rigid in your response. You must have a flexible playbook framework. ■

“A business impact analysis will help you know what’s important to the business.”

In newer or less mature environments, people talk about focusing on critical elements, but how do you know what those critical elements are? You can approach this question from either the inside or from the outside.

A business impact analysis will help you know what’s important to the business. What are the critical elements in the business? What do you most need to protect? What is critical to the survival of the business? The result of that analysis generates a priority list.

From the outside, you have to know which attacks are currently in play. Publications from major vendors review the incident response activities they went through without specifying customers.

These documents may say something like, “In the past year, we’ve handled 500 or 1,000 breaches. Over those breaches, we saw these five or six things continuously. Customers are still not taking care of them, and that’s why they’re getting breached.” Look at what the bad actors do most often, correlate that against the (internally generated) priority list — what’s important to your business — and concentrate on protecting the most important parts of your business against those attacks. That approach will help you prioritize security improvements. ■

Dmitriy Sokolovskiy, Chief Information Security Officer, Avid Technology

Since 1999, Dmitriy has consulted defense contractors, financial and medical companies, and nonprofits. In 2007, he created CyberArk’s Implementation Services teams, and personally participated in the largest breach remediation events. In 2016, Dmitriy was the SaaS product Cloud Security Architect, and in 2018, Dmitriy became the CISO for Avid Technology, where he advises information security start-ups, and venture capital firms. Dmitriy is also a member of the GIAC Advisory Board and holds the GISF, GCED and CISSP certifications.

Felipe Medina, VP of Information Security Architecture and Operations, BankUnited

Felipe Medina is responsible for establishing and maintaining a corporate-wide information security technology program to ensure that information assets are adequately protected both on premises and within multiple cloud environments/ technologies. This includes having an up-to-date understanding of the latest security threats, trends, and technologies, managing and supporting existing security solutions, evaluating, designing, and implementing new technical security controls, and working to meet security objectives.

"When you go with a more SaaS-based or cloud-native solution, you're focusing on becoming a refiner and consumer of that data and platform."

Consider the cost of maintaining agents' updates, platform updates, and troubleshooting issues with servers or network communications. You can go with a brick-and-mortar solution that does well, but you're not factoring in the amount of upkeep and maintenance required. When you go with a more software-as-a-service (SaaS) – based or cloud-native solution, you're focusing on becoming a refiner and consumer of that data and platform. Gone are the days of constantly patching servers. Ask yourself, What's the result instead of that patch? What's the result instead of what you're introducing into the environment with a new policy?

Instead, create a baseline of what you're doing with a SaaS platform. Then, you become a consumer and refiner of that data, but you're not necessarily bound to that platform. That's one factor that I would say security leaders need to consider, especially if they have a small security team. The smaller your security team, the more painful it will be to stay ahead of that threat-hunting and threat intelligence piece. Making fundamental changes — including mindset changes to make us a more cloud-native organization — enabled us to get ahead of the curve.

“Consider getting external help to manage this process, such as contracting with an MDR provider or MSSP.”

The right tools for incident detection and response are essential. Make sure that you can rapidly deploy any configuration changes remotely. Consider getting external help to manage this process, such as contracting with an MDR provider or MSSP.

This pandemic has shown us a magnitude of scale we have never seen before. To my surprise, most enterprise cloud providers were able to handle the increased load, although we discovered that provisioning or onboarding thousands of users can be a daunting task. Therefore, plan for that scenario, with contracts to help you scale.

From another viewpoint, you could say that nothing changed with the pandemic. You must still focus on what is most important to the business, which begins with understanding how your program supports your business objectives. Your security projects should focus on specific business outcomes rather than attempting to address fear, uncertainty, and doubt, as they have in years past. You can’t solve every problem, so find the top twenty percent that addresses 80 percent of your risks. When you’re done, move to the next 20/80 rule. ■

Genady Vishnevetsky, Chief Information Security Officer, Stewart Title

Genady Vishnevetsky serves as the Chief Information Security Officer (CISO) for Stewart Information Services Corporation, a leading provider of real estate services, including global residential and commercial title insurance, escrow and settlement services, lender services, underwriting, specialty insurance, and other solutions that facilitate successful real estate transactions. An established leader with experience in building a successful security program and developing the defense against emerging threats, Vishnevetsky leads the security, governance and compliance program for the global enterprise.

Matthew Otwell, Chief Information Security Officer, MD Department of Health

Matthew Otwell has been an IT and Information Security professional working with multiple global or state organizations over a 25-year span. Currently, Mr. Otwell serves as the CISO for the MD Department of Health. His educational background includes a Bachelor of Science in Electronics Engineering Technology from Capitol University and multiple certifications including CISM (Certified Information Security Manager), CCSK (Certificate of Cloud Security Knowledge), and ITIL v.3 Foundation.

"Now, our eyes are open. We've begun to think about the possible scenarios instead of just the probable ones."

Consider the worst-case scenario. Most organizations typically plan only for the 50th percentile. For example, for the remote workforce, they may think, "In some situations, maybe half our workforce will be at home, and the other half of the workforce can still access the building." From a disaster-recovery perspective, that approach may work well if you have other buildings or other areas in which people can do their work. That's taking a localized approach to business continuity.

As a former chief security officer once told me, however, it's our job as security leaders to think about what is possible, and then determine the probability. You still have to plan for both. There was a time when organizations could rely on that localized business continuity approach. Today, we better understand what business continuity means to each organization from a global perspective.

Now, our eyes are open. We've begun to think about the possible scenarios instead of just the probable ones. We can begin to establish more flexible plans that can adapt to each scenario. Again, I come back to that good information security framework. As long as the foundation is solid, you can customize the other elements to fit your scenario. ■

“When you’re moving from one technology to another, you may experience additional threats because the current situation makes you move a little faster or in a different direction.”

The most important thing is to keep up on the latest technology. There’s always some new tech, some new tool. When you’re moving from one technology to another, you may experience additional threats because the current situation makes you move a little faster or in a different direction. That’s when you want to bring in your partners and talk to your peers. Ask them, “Hey, what are you doing about this? How are you solving this problem?” Talk to Gartner, your peers, and other analyst firms. Try to understand what really matters.

It’s important to be aware of the threats and the technologies available to address them. You don’t have to do it all yourself: You may have a security architect who can do it for you, for example. Some companies I’ve worked with have offered threat assessment as a service — for example, if you have a specific need, they hunt down four or five companies for you. Then, those companies present their product based on your requirements, saving you time. Be savvy when undertaking such tasks.

Nikk Gilbert, CISO, Confidental

With 20 years of executive level experience in information technology roles, Nikk is a respected thought leader within the government & private sectors. Nikk holds the CISSP and CISM security certifications and has been a keynote speaker at technology events throughout the world.

CHAPTER 5

STAYING AHEAD OF CHANGE

Finally, building a flexible threat-detection and response strategy comes with its own challenges. Can the security team accomplish all its priorities in house and still account for the necessary business continuity planning, or is it time to engage outsidehelp? What are the best practices when doing so? How can you ensure that you have the most resilient threat-detection and response strategy possible for eradicating threats in 2020 and beyond? With that in mind, we asked security experts the following questions:

How do you define your use cases and security outcomes?

How do you determine when to seek help from an MSSP?

What advice can you offer security leaders who are considering a partnership with an MSSP versus an MDR provider for threat detection and response?

David Van, Investors Bank, VP InfoSec Engineering and Operations

An information security professional with a demonstrated history of working in the banking industry. Skilled in IT infrastructure management, cloud security, information security, IT Infrastructure operations, and virtualization. Strong operations professional with a Bachelor of Arts in Mathematics and Computer Science from Binghamton University. Security certifications include CISSP and CCSP.

“Measurement is where the MDR provider can shine because it should come out with trending metrics, such as key risk indicators and key performance indicators”

In addition to what I shared earlier, say that you selected an MDR provider based on your specific criteria. For example, you may need more anomaly detection because of your industry, or you may need an MDR provider that can help you comply with privacy regulations. Now that you’re working with the MDR provider, the next question is, How do you measure your success? Measurement is where the MDR provider can shine because it should come out with trending metrics, such as key risk indicators and key performance indicators.

It’s the MDR provider’s job to prove to you, as the enterprise that engaged it, that the provider’s staff are continuously collecting the data you need. Say you have 1,000 endpoints — 1,000 employees now spread across America. You want the MDR provider to show you, with numbers and graphs, that you are getting approximately 1,000 sources coming in and feeding the analysis engine. You should have visibility into all of them. If the MDR provider is showing you a report on 100 endpoints, what happened to the other 900? This is why you’re relying on the MDR provider: to give you insight into trends based on these metrics.

Deneen DeFiore, Vice President & Chief Information Security Officer, United Airlines

Deneen DeFiore is VP and CISO for United Airlines. She is responsible for shaping United's cybersecurity strategy to ensure that the company is prepared to respond to evolving cyberthreats and regulatory obligations. She also leads the company's initiatives on commercial aviation cybersafety risk and improving cyber resilience. She works with industry partners to reduce cybersafety risk worldwide across the aviation ecosystem.

"Defining your use case and security outcomes starts with understanding your business goals and outcomes."

Defining your use case and security outcomes starts with understanding your business goals and outcomes. What is your business trying to accomplish? That's what you're there to protect. That answer will inform where you need to go, and the direction will vary depending on the type of business. For example, the threat profiles and security approaches of a large defense contractor are going to look different from those of a commercial retailer.

Also consider the capability of your team or the availability of resources within your market area because there's always a shortage of cybersecurity talent. If you are going to need skilled resources and you don't have them, that's when you can think about augmenting your capabilities with an MSSP or MDR provider.

I've been in my chief information security officer role at United for less than a year, and I'm looking at the capability needs for my organization. In my opinion, MDR providers offer solutions more tightly integrated with technology and detection and response. MDR providers offer intelligence technology, and their staff are an extension of your team so you don't have to find specialists. They could be a better play for organizations that don't have a lot of capital to invest in technology or the resources to support and maintain security technology over time.

“When do you choose to use an MSSP or an MDR provider? The answer is based on a combination of requirements and resource availability.”

When do you choose to use an MSSP or an MDR provider? The answer is based on a combination of requirements and resource availability. If the requirement is 24/7 coverage or 20/6, for example, staffing can be expensive. For a single operations center role, you need a minimum of four people, and then it goes up from there. You also need to build in the cost of the locations. If you’re not a large company, that investment can be cost prohibitive. That’s when you start looking at MSSPs and MDR providers.

If you decide to engage an MSSP or MDR provider, you have to determine the level of coverage you really need. With MDR providers, you must also be clear about what you want the provider to do. Half of these providers will note, investigate, report, but not act. Are you OK with that? Do you want the provider to act? What kind of action do you want? Should the provider’s staff actually go into your machines and start clearing things out? Do you want them to trigger some form of security orchestration capability? Do you want them to develop such a capability as they go? Those are the things you want to put in the fine print of your contract with the provider. ■

Dmitriy Sokolovskiy, Chief Information Security Officer, Avid Technology

Since 1999, Dmitriy has consulted defense contractors, financial and medical companies, and nonprofits. In 2007, he created CyberArk’s Implementation Services teams, and personally participated in the largest breach remediation events. In 2016, Dmitriy was the SaaS product Cloud Security Architect, and in 2018, Dmitriy became the CISO for Avid Technology, where he advises information security start-ups, and venture capital firms. Dmitriy is also a member of the GIAC Advisory Board and holds the GISF, GCED and CISSP certifications.

Felipe Medina, VP of Information Security Architecture and Operations, BankUnited

Felipe Medina is responsible for establishing and maintaining a corporate-wide information security technology program to ensure that information assets are adequately protected both on premises and within multiple cloud environments/ technologies. This includes having an up-to-date understanding of the latest security threats, trends, and technologies, managing and supporting existing security solutions, evaluating, designing, and implementing new technical security controls, and working to meet security objectives.

"Any MSP, whether it's an MSSP or an MDR provider, has to be an extension of the organization."

Any managed service provider (MSP), whether it's an MSSP or an MDR provider, has to be an extension of the organization. That provider must be empowered to the extent possible to provide the services you have engaged it to provide. It should be clear to everyone involved what that provider's goals are. Defining the goals for an engagement with an MSSP or MDR provider requires a certain level of maturity within your organization. Your organization must know what it's going to request or understand what the MSSP or MDR provider offers so that it can provide the MSP with clear guidance.

If that understanding is not in place, then your service won't be as fruitful as it would be if you had said, "This is what I need from your service, and this is what the goals are. This is what you will have the power to do, and this is what you won't have the power to do." I've seen time and again that MSSPs and MDR providers are thrown under a bus because the organization doesn't know what it wants. Before you go to an MSSP or an MDR provider, therefore, understand what you're trying to solve and why you need this partnership.

“Your decision to seek help from an MSSP should be driven by business objectives and priorities.”

When it comes to defining your use cases and security outcomes, map your use cases to the MITRE ATT&CK framework. Know and understand your adversaries: They may be different from your allies or competitors. Focus on detection because protection can only go so far.

Your decision to seek help from an MSSP should be driven by business objectives and priorities. Do you need 24/7 coverage? Do you have the right level of expertise on your security team? What kind of visibility and coverage do you need? Your answers to those questions will determine your requirements for managed service.

When it comes to working with an MSSP versus an MDR provider, the choice depends on what you are trying to accomplish. MDR focuses on the incident detection and response based on specific tools deployed on the endpoint; MSSPs take a holistic view that encompasses everything. Where are your gaps? Keep in mind, managed services is a marriage, not dating, so establish a relationship before making a commitment. Understand that all managed service providers will have limitations. They can’t accommodate every customer request. Weigh the limitations against your level of comfort and risk.

Set up a weekly cadence meeting. Establish metrics and key performance indicators that matter to your business, and report them to your board of directors. The number of failed sign-ins or closed tickets is irrelevant. Choose metrics that reflect your security posture and justify the MSSP contract. Measure the return on your engagement investment.

Genady Vishnevetsky, Chief Information Security Officer, Stewart Title

Genady Vishnevetsky serves as the Chief Information Security Officer (CISO) for Stewart Information Services Corporation, a leading provider of real estate services, including global residential and commercial title insurance, escrow and settlement services, lender services, underwriting, specialty insurance, and other solutions that facilitate successful real estate transactions. An established leader with experience in building a successful security program and developing the defense against emerging threats, Vishnevetsky leads the security, governance and compliance program for the global enterprise.

Matthew Otwell, Chief Information Security Officer, MD Department of Health

Matthew Otwell has been an IT and Information Security professional working with multiple global or state organizations over a 25-year span. Currently, Mr. Otwell serves as the CISO for the MD Department of Health. His educational background includes a Bachelor of Science in Electronics Engineering Technology from Capitol University and multiple certifications including CISM (Certified Information Security Manager), CCSK (Certificate of Cloud Security Knowledge), and ITIL v.3 Foundation.

"If you can identify when you've hit that overflow point, that is the best time to engage an MSSP."

Most security leaders understand what it takes to accomplish specific security goals and outcomes. It is difficult, however, to recognize when things are beginning to spiral out of control. Often, we don't see that we're getting in over our heads until it's too late. We need the knowledge and the fortitude to recognize when things are beginning to overflow.

If you can identify when you've hit that overflow point, that is the best time to engage an MSSP. Doing so after the fact could be extremely difficult: You don't know what the timeline is, and you don't know what other commitments the MSSP may have. If you can establish the turnaround you need from a specific MSSP for specific services, then you can determine whether to engage that MSSP in a retainer agreement or for a short-term contract.

Make sure that the MSSP is committed to a partnership with your organization, not just providing a service. If your business relationship with an MSSP is strictly transactional, then that MSSP is not going to go the extra mile or provide that value-add in your time of greatest need. Ideally, the partnership should be mutually beneficial.

“Start with a scoping gap analysis. Then, bridge that gap and mitigate that risk.”

When considering whether to work with an MSSP or an MDR to build and implement a flexible threat-detection and response strategy, it really comes down to how many people you have, how much work you have to do, and the level of expertise your people have.

Start with a scoping gap analysis to figure out whether you have the people you need to get the job done and whether those people have the knowledge and skills to do it. Then, bridge that gap and mitigate that risk. This step is especially important if you’re working with a new technology and don’t have anyone in house who knows it well enough. In such a case, consider bringing in a third-party provider to fill that gap.

Whether you decide to work with an MSSP or an MDR also depends on the maturity of your program, the maturity of your security leader, and the expertise of the team. There are many pieces of the puzzle to consider when making the decision. ■

Nikk Gilbert, CISO, Confidental

With 20 years of executive level experience in information technology roles, Nikk is a respected thought leader within the government & private sectors. Nikk holds the CISSP and CISM security certifications and has been a keynote speaker at technology events throughout the world.

Eradicate Hidden Threats

Transform your threat detection and response strategy to protect against advanced threats that may already be in your environment.

Hunt for Threats Today

Trustwave®