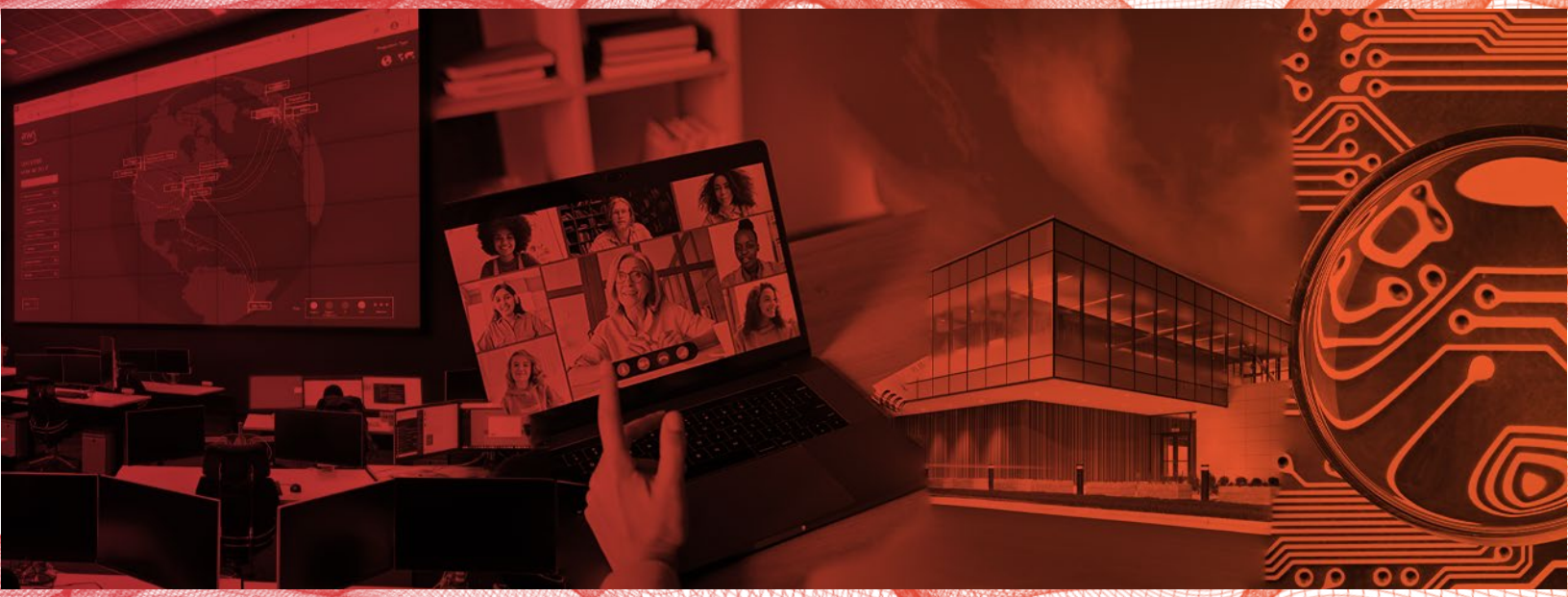
HERJAVEC GROUP + fishtech group

2022 CYBERSECURITY CONVERSATIONS REPORT



Cyber Resiliency for the Evolving Threat Landscape

HERJAVEC GROUP + fishtech group

2022 CYBERSECURITY CONVERSATIONS REPORT

Contents

A Message from Robert Herjavec

Welcome to 2022!

In last year's Cybersecurity Conversations Report, we discussed what the massive digital transformation resulting from 2020 meant for enterprise cybersecurity. We encouraged enterprises to prepare for the post-COVID paradigm shift by prioritizing:

- "COVID" Testing Your Devices
- Refreshing Emergency Preparedness Plans
- Reprioritizing Scanning and Testing Programs

Last year I went on record predicting 2021 to be the most profound year in cybersecurity history. This proved absolutely true - but not necessarily in all the ways we expected.

In last year's report, we predicted a mass move back to the office. What we learned instead is that we will likely never return to the physical perimeters of the office as we knew them in the past. While some companies started the transition back to the office, most realized that a hybrid of remote and in-person work is here to stay. This fluid dynamic presents a particularly complex challenge for enterprise security teams that will need to be addressed with a combination of legacy and innovative methods.

What we did see come to fruition in 2021 was an unprecedented increase in frequency and sophistication of cyber-attacks. Ransomware was more pervasive and more disastrous than ever before. We witnessed attacks impacting critical infrastructure, enterprises, and individuals alike. But while there was a lot of attention and fear surrounding cybersecurity, the events of 2021 resulted in some really encouraging moments in our industry as well.

Government support for programs and regulations that aim to prevent and intervene in cyber-attacks is at an all-time high. CISOs and infosec professionals are finally getting a seat at the table at an executive and board level. We're even starting to see programs educating kids about the importance of cybersecurity –

What we did see come to fruition in 2021 was an unprecedented increase in frequency and sophistication of cyber-attacks.

nurturing interest and awareness at an early age. These are all reasons to feel very hopeful and excited for the future of our industry!

That being said, there's a lot of work to be done. If we've learned anything in the past two years, it's that waiting for things to return to normal simply isn't feasible – because they likely never will. The new normal in cybersecurity is one that demands resiliency and the ability to rapidly pivot and adapt. We must learn to be effective and productive in the chaos.

We can no longer continue "just getting by". This means learning to embrace the chaos rather than pushing against it. Everything has changed – and while that notion can be scary, it also brings with it a huge amount of opportunity ! Never before has cybersecurity been so prominent on the world stage. People outside of our industry are finally understanding the importance of cybersecurity – and the consequences of neglecting it. Now is the time - while the whole world is sitting up and listening – to build your enterprise cybersecurity into an effective, resilient program that not only secures your company, but drives business.

Speaking of big changes and big opportunity – the recent merger between Herjavec Group and Fishtech Group has resulted in a roster of best-in-class talent and service offerings that I couldn't be more excited about. Our combined organization brings together world-class talent and extensive expertise. As the new security solutions powerhouse, we are perfectly positioned to take on the cyber challenges of 2022 and beyond. For this report, we surveyed our executive team for their unique insights into how enterprise leaders should adapt their cybersecurity programs to address the threat landscape ahead.

This year, our Cybersecurity Conversations for the C-Suite Report is dedicated to the conversations we recommend having with your executive teams in order to build cyber resiliency for the evolving threat landscape:

- Adapt your program to embrace the constant change
- Investing wisely in your cybersecurity program
- Taking a security-oriented approach to your business

As we move into 2022, ask yourself:

- Do I know where my current enterprise cybersecurity posture stands?
- Is my cybersecurity program robust enough to secure a hybrid workforce?
- What endpoint security measures do I have in place to ensure full visibility?
- Do I know what my specific cybersecurity needs, gaps, and risks are?
- Have I engaged all the right stakeholders within my organization to build a comprehensive cybersecurity program?
- Is cybersecurity seen as a business barrier or a business driver in my organization?

If you don't have complete confidence in answering these questions, you're likely unprepared to face the cyber challenges ahead.

2021 may not have been the year we expected, but the events of the past year have left reason to be hopeful. With great change comes great opportunity. I've seen our cyber community come together and bolster each other in ways we never could have imagined. I'm grateful to be part of an industry that serves such a profound and growing purpose and I can't wait for what's ahead.

Here's to a (cyber) safe 2022…

Let's keep the conversation going.

To your success,

Robert Herjavec

Embrace the Constant Change

There's no denying it – remote and hybrid workforces are here to stay. Since the mass digital transformation began in 2020, organizations all over the world have been forced to accommodate a work-from-anywhere approach. In short, we spent the last two years reacting. IT teams across the globe deserve a standing ovation for the incredible work they did rapidly moving business operations online in 2020. Security teams deserve one for facing the constant and rampant cyber-attacks in 2021. While this reactive, adrenaline-filled approach helped get us through these unprecedented times, it simply isn't sustainable in the long-term.

For the past two years, most IT and security teams have been waiting for things to "settle down" or "go back to normal" to start thinking about long-term strategies. Let this serve as a gentle wakeup call – things may never settle down and if we have learned anything from the past two years, it's that what we deemed "normal" will likely never return. We as a cyber community must come to terms with the fact that we will never "catch up" if we continue with the same approach. Things are changing every day. So how do we face the continuously evolving threat landscape?

The answer is a resilient cybersecurity program that can rapidly pivot and adapt. This will require:

Agility

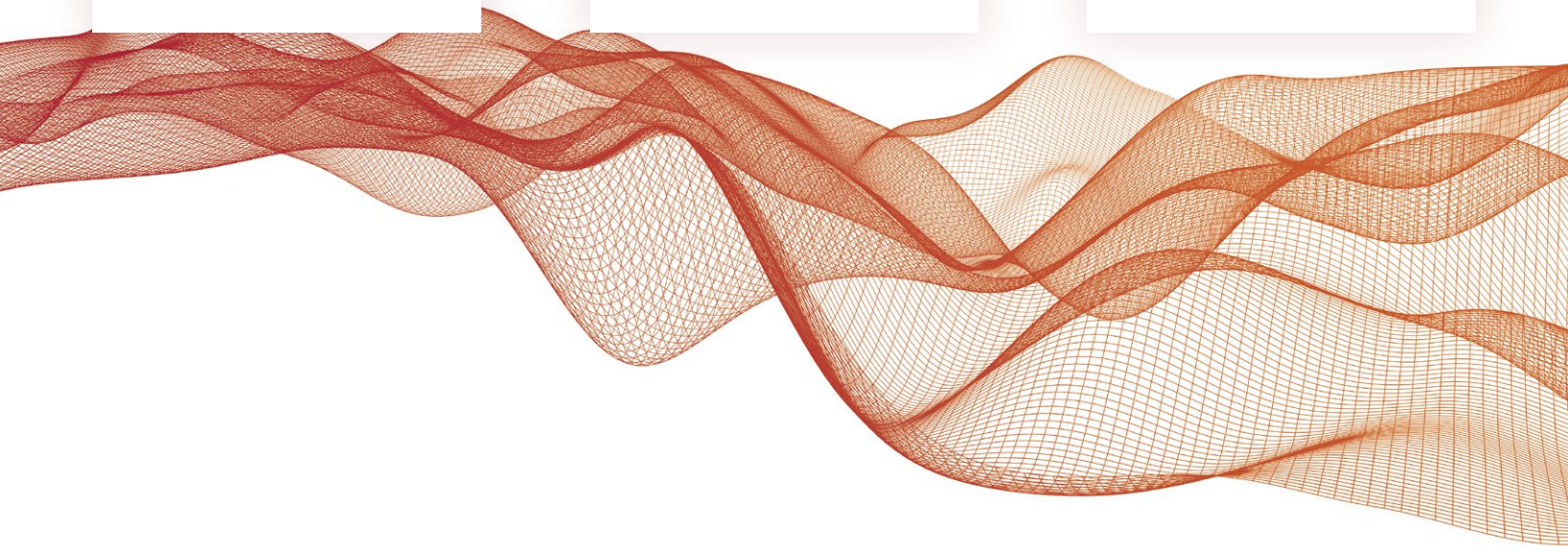
Constant assessment and improvement to evolve with the threat landscape.

Visibility

Identifying all endpoints, risks, and vulnerabilities and know which to prioritize.

Preparedness

Having an incident response and post-mortem plan ready before a breach occurs.



Agility

The crux of a strong cybersecurity program is its ability to change with the times and continuously improve. Threat actors are constantly working to outsmart cybersecurity programs. It's up to you and your team to stay one step ahead of them. The best way to do this is to constantly test, iterate, and improve your cybersecurity program.

Not sure where to begin? Start by developing a continuous improvement plan that includes a balance of manual and automated tools.

Red team operations and penetration testing use real-world adversary tradecraft to assess your security posture. The ultimate goal of both assessments is to test the security posture of your organization as well as your complete stack of security controls, specifically by using adversarial tactics.

VP of Customer Success, Eric Dowsland recommends also considering simulation tools to validate the work your security team does on an ongoing basis. Breach Attack Simulations can be used to validate controls managed by security engineers, ensure current detection mechanisms are catching inappropriate behaviours, and can even reduce the spend on other efforts like Red Teaming or Pen Testing.

Mixing these manual tools with the automation of Vulnerability Management is a great way to identify potential vulnerabilities before they become security incidents.

Vulnerability Management is one of the best ways to identify indicators of coverage, control, and overall security within your security program.

A strong Vulnerability Management program allows organizations to identify potential security gaps including access points that threat actors can leverage to gain entry into corporate networks and then prioritize these vulnerabilities for remediation.

However, building a robust vulnerability management program can be complex and isn't without its challenges. Eric notes "vulnerability management programs that aren't optimized to achieve desired results based on your enterprise's unique cybersecurity needs can be wasteful of your team's time and effort, not to mention your investment."

Not sure where to begin?

Start by developing a continuous improvement plan that includes a balance of manual and automated tools.

Eric suggests focusing on the 5 key components of a strong Vulnerability Management program:

1 Asset & Vulnerability Discovery

Organizations need to know where they have technology deployed, even in scenarios where remediation might not be possible or easy. It's important to always understand the "surface area" of your organization. Security teams should work closely with infrastructure and operations teams and all application and asset owners to ensure blind spots are identified and addressed.

Scanning is also critical for a vulnerability management program. While there are subtle differences in the leading scanners, all use the NIST CVE Data and will generate some form of score based on the Common Vulnerability Scoring System (CVSS).

Ensure that your scanning solution:

- Has a proven track record in your specific industry
- Can demonstrate the ability to do custom scanning profiles for different parts of the organization
- Keeps up to date on the CVE Database

Scanning regularly and at a time that is optimal for the remediation cycle is also key. Schedule regular scanning based on your organization's risk tolerance, compliance mandates, and the number of other asset classes.

2 Vulnerability & Risk Prioritization

Most organizations have a threshold for the time taken to patch based on the Common Vulnerability Scoring System (CVSS) score of the vulnerability. However, emphasis should be placed on prioritizing which of the high and critical vulnerabilities are most likely to compromise your environment.

The key question with managing vulnerabilities should be around data enrichment. What can your security team do that will enhance the raw vulnerability data to effect precise risk-based decision making? Implement a strategy that optimizes your team's efforts and ensures they are addressing vulnerabilities that are relevant, exploitable, and are a significant business risk.

> "Vulnerability management programs that aren't optimized to achieve the desired results based on your enterprise's unique cybersecurity needs can be wasteful of your team's time and effort, not to mention your investment.
>
> Craig Jett
> SVP, Consulting & Professional Services

3 Patch Management

The biggest challenge in Patch Management is that the patching policy often competes in priority with other IT or business initiatives. The security team may end up being a "drag force" in moving the business forward. Three components help alleviate this drag force:

1. Risk-Based Vulnerability Management as defined earlier helps reduce the noise and provides IT more precision and efficiency on what to patch and how critical the patch is.
2. Integrate your vulnerability management platform with your IT Service Management (ITSM) platform.
3. Understanding that patch management is not the only treatment available for addressing vulnerabilities. Other approaches that may be less ideal from a pure security perspective can enable business operations while still addressing the vulnerability. This includes leveraging compensating controls and risk acceptance, configuration changes and system hardening, and network segmentation, to mitigate the risk of vulnerabilities.

4 Remediation & Exception Tracking

Some well-run vulnerability management programs have provisions for self-service scanning. This is particularly helpful in environments where there's an application development that spits out code faster than the normal scanning interval would be able to keep up with. In this scenario, on-demand scanning can be valuable for validating whether a vulnerability has been patched or not in.

5 Actionable Metrics

Meaningful and quantitative metrics can justify and quantify your actions, decisions, and resource utilization while also helping you identify your vulnerability management program's shortcomings.

Focus on operational and executive metrics that measure performance, prompt actions, and convey the value delivered by the vulnerability management capability. This could include:

- Average days to patch critical systems with critical patches
- Percentage of vulnerabilities that were unable to be patched
- Number of security incidents caused by exploited vulnerabilities
- Investments to support faster or slower patch times

Taking an action-oriented approach to communicating your metrics will help gauge progress and give a clear path to deal with a status that isn't ideal.

Ask yourself:

- What scanning and testing tools am I leveraging? How often am I implementing them?
- Do I have a Vulnerability Management Services in place?
- How do I validate updates?
- Am I meeting industry and government guidelines?
- What is the number of vulnerabilities that meet the crux of being critical or exploitable, on essential assets?
- What metrics am I using to justify and quantify my actions and decisions? Am I communicating them to the right demographics?

Visibility

Today, comprehensive visibility is essential for any organization's cybersecurity program. It also happens to be increasingly complex and tedious to achieve and manage. As our Chief Product Officer Atif Ghauri concisely describes it, "the proliferation of identities is complicating enterprise security strategy, but identifying and securing those identities it not an option."

With hybrid and work from anywhere work environments, security teams are not only tasked with identifying all the organization's end-users, but they also must understand what they are doing with the accounts and access they have.

Human beings, devices and applications all have identities. It is imperative that your enterprise not only has visibility across all three categories, but is also effectively managing security controls for each one.

Our SVP, Identity & Access Management, Todd Musselman explains that "remote and hybrid work 'at scale' have certainly complicated this effort as behavior patterns have shifted significantly because of the pandemic. People are logging on at all hours of the day, their kids are using their corporate devices, personal emails are being accessed and the list goes on. The opportunities for hackers to take advantage of these new vulnerabilities are endless."

Todd also notes that compromised identities continue to be the primary mode of attack for cyber adversaries. "Compromised credentials can be used to break into a network, move laterally within the network, and facilitate all kinds of damaging activity. Identity should be at the top of your list of prioritized security focuses."

The complexity of digitally transformed enterprise environments, including the diverse set of endpoints/ identities and internal and external/third party access, have resulted in increased vulnerabilities and opportunities for threat actors.

The Key Pillars of Identity

Identity Governance & Administration (IGA)

IGA is the policy-based centralized orchestration of user identity management and access control. These tools manage digital identity and access rights across multiple systems by aggregating and correlating disparate identity and access rights data that is distribute throughout the IT landscape to enhance control over user access.

According to **Gartner**, this aggregated data serves as the basis for core IGA functions, including:

- Identity life cycle management
- Entitlement management
- Access requests
- Workflow orchestration
- Access certification (also called "attestation")
- Fulfillment (also called "provisioning") via automated connectors and service tickets
- Reporting and analytics

In a mature IAM program, IGA tools leverage data sources and complement access management. It can also provide support with role and policy management, password management, and auditing.

Privileged Access Management (PAM)

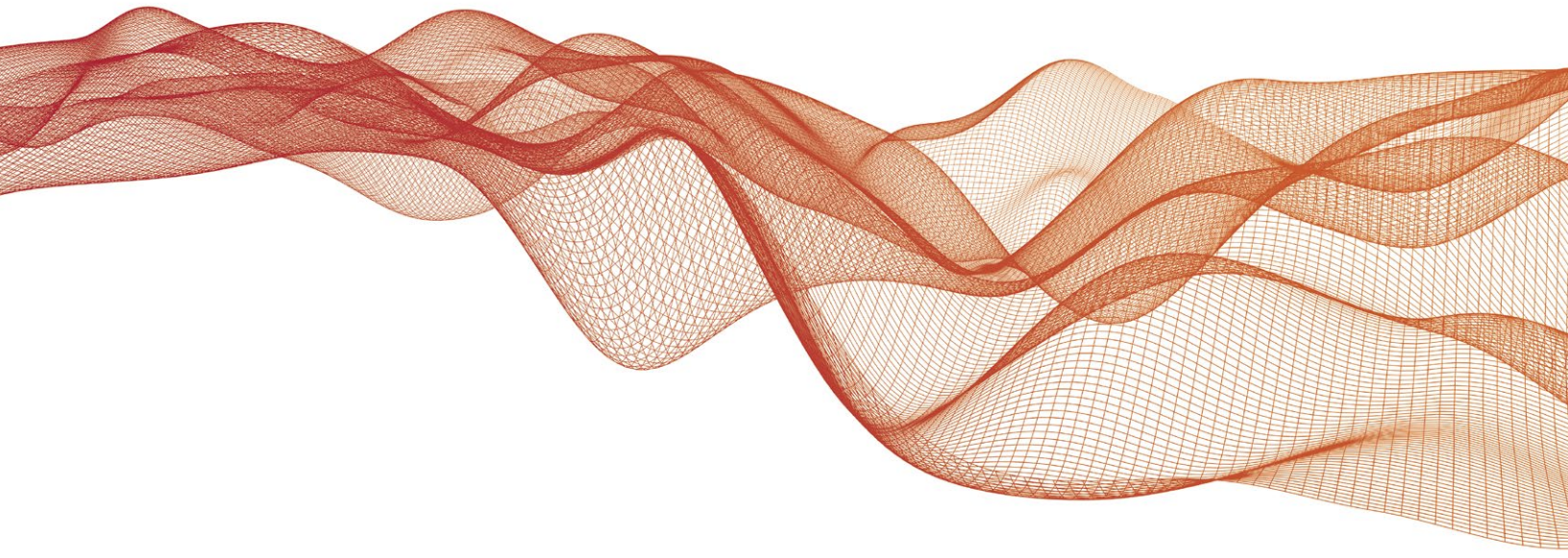
PAM tools provide secure, privileged access to critical assets to only the intended users, and meet compliance requirements by securing, managing, and monitoring privileged accounts and the related access.

An effective PAM program will allow you to:

- Identify unusual end-user behavior that could signify malicious activity
- Give necessary privileged access to internal and external parties
- Systematically de-provision those who don't require privileged access

Implementing a strong PAM program can address many of the challenges organizations face when dealing with privileged access:

Problem	Solution
Lack of policy and standards that define requirements for protecting and managing privileged accounts	Customized roadmap and strategy plans, standards, RACI chart, and prioritization/risk models
Need for assistance with upgrading, installing, or implementing health checks of PAM software and platforms	Expert guidance with design, architecture, review, and deployment of PAM tools
Penetration Test and audit findings that indicate a compromised privileged account, 'pass the hash' vulnerability, or failure to meet PAM-related controls	Set strategy and support deploying solutions to remediate findings
Inability to manage privileged credentials used in the DevOps pipeline	Support securing privileged credentials for the DevOps pipeline using PAM tools to remove hardcoded credentials and authenticate applications using granular access controls
Improper storage of credentials using high risk processes run by RPA bots using credentials managed by RPA platforms	Expert support for enterprise IT and business administrators to define scope of privileged access and accounts that should be managed in a PAM tool platform
Inability or lack of formal process to rotate service accounts or other application/system credentials	Access to experts with experience in a variety of workflows to manage application credentials
Difficulty securing and managing third-party access to internal systems	Managed PAM tools leveraged to manage remote vendors by providing just-in-time privileges using multifactor authentication



User Authentication and Access Control

User authentication is the real-time corroboration (with an implied or notional confidence level) of a person's claim to an identity previously established to enable access to an electronic or digital asset.

Traditional authentication and access control processes are no longer enough to keep up with the current cyber threat landscape due to negative user experience, failure in consistency throughout an organization, and outdated systems.

VP, Identity & Access Management, Doug Chin suggests building User Authentication and Access Control programs that are centered around the user, as opposed to networks, devices, or endpoints. "This allows you to gain both greater internal visibility and a better understanding of the customers and the products and services that they use."

Doug also explains that developing a cybersecurity strategy that balances risk mitigation and user experience is key. "You can have the most sophisticated cybersecurity tools on the market but without buy-in from all end-users, your cybersecurity program would be useless. It's about balancing endpoint resiliency and secured continuous access."

Your User Authentication and Access Control program should include:

- Accessible cybersecurity training and education for employees at all levels of your organization
- Tools that mitigate risk while not being a barrier for the end-user
- Support for employees to practice good cyber hygiene including time to update software on a regular basis

Resilient Third-Party Risk Management is No Longer an Option

Historically Identity & Access Management programs were seen solely as a risk solution for an organization's internal team. However, as recent events have shown us, entities that exist outside the business are equally vulnerable to system threats. As we've seen an increase in third-party breaches, we've been reminded that technological advancement will always carry inherent risks. The SolarWinds breach served as a tough lesson that today, security visibility must extend past our internal team.

In the wake of the pandemic, we continue to see rapid digital transformation – including big changes to the way enterprises require and engage third parties. One thing is certain: it's more difficult than ever to define and identify third parties and you can't protect your enterprise against something you can't identify!

Before the pandemic, the typical network security perimeter made it easy to differentiate between our teams and external users. Today, the way we give access to our employees is generally the same way we give access to third parties. Without a mature security program, this can lead to some messy and sometimes catastrophic situations.

SVP, Identity & Access Management, Todd Musselman suggests developing a structured practice starting with your Legal and Compliance teams to ensure the right privileged access is given and only for the necessary amount of time. The process should include a thorough assessment of all potential third-party vendor cybersecurity. "When engaging a third party, ask questions and look for indicators of best cybersecurity practices that align with yours. Developing streamlined processes to address external end-user vulnerabilities will free your security team to focus on critical risks."

Third-party risk is present with any external end-user that has access to your network – from the vendors that directly contribute to your business to peripheral services like office maintenance.

Finally, ensure your Identity Governance and Administration, Privileged Access Management, and User Authentication and Access Control programs include third-party users. Your team should have a clear understanding of the cascading effects of cybersecurity in your supply chain – including the trickle-down consequences of a breach.

Ask yourself:

- Do I have visibility into how privileged access is being used?
- How am I enforcing my enterprise password policy for privileged accounts?
- Does my team have the ability to detect and respond to threats against privileged accounts?
- What is my process for ensuring third-party end-users leverage best cybersecurity practices that align with mine?

Preparedness

In 2021, you couldn't look through your newsfeed without seeing something about a ransomware breach. Craig Jett, SVP, Professional Services notes that "the ransomware we are seeing today is multifaceted and much more targeted. It's coming from many directions and targeting specific individuals." While there's a lot of fear and uncertainty surrounding ransomware, there are many ways you can prepare your team.

The worst time to decide what to do about an incident is after it occurs. When it comes to a cyber breach, time is truly of the essence. The longer a threat actor has has access to your system, the more time they have to cause damage, and the more the cost of the incident increases. Planning how your security team will address a breach will ensure you don't lose precious time deciding what to do.

$3.92 million

The average cost of an enterprise data breach.

(CSO Online)

7 Steps to Mitigate Ransomware Damage

Principal Consultant, Consulting Services, David Mundhenk, explains that "while some teams are proactive enough to obtain and deploy state-of-the-art malware prevention software and systems, many may fail to 'complete the last mile' in this process – preparing with robust Incident Response policies plans, and programs in the event of a ransomware attack.

If you're not sure where to begin, start by considering these 7 actions that can significantly enhance security organizational maturity and capabilities in the face of a ransomware attack:

1 Make Sure Your Incident Response Strategy Covers Ransomware

Check that Incident Response policies, processes, and procedures include ransomware and malware detection and response capabilities.

2 Prioritize Post-Incident Review and Continuous Improvement

Incorporate a post-attack evaluation after any ransomware or general malware outbreak and ensure that lessons learned are incorporated into existing capabilities.

3 Prepare for the Worst by Backing Up

Regularly back up all critical systems and data to a secure archive. Take inventory and test all system backups on a regular basis to ensure their viability to aid in recoveries in light of a ransomware attack. Also, keep in mind that some of those system backups may also become infected with malware during a breach. Be sure to enhance capabilities to validate backup integrity.

4 Ensure Your Whole Team Knows How to Detect and Report Potential Ransomware

Enhance security awareness training for personnel and ensure a primary focus on how to detect and report possible "phishing" attacks that could deliver different forms of malware including ransomware.

5 Segment and Isolate Your Crown Jewels

Enhanced network segmentation controls can aid in slowing, or even stopping many forms of malware outbreaks including ransomware. Review network configurations and controls. Use the results to develop enhanced network segmentation and isolation for critical information assets, sensitive data, and the systems they run on.

6 Make Sure Detection and Response Tools will Cover Ransomware

Review and enhance network firewall and IDS/IPS capabilities to detect, alert and respond to suspected malware-induced network traffic.

7 Prepare with the All Necessary Parties

Consult with corporate legal counsel and business risk insurance companies on how best to respond to a possible malware outbreak before one occurs. Keep in mind that many insurance companies are starting to refuse payoffs for malware claims.

Investing Wisely in Your Cybersecurity Program

American investor and entrepreneur, **Reid Hoffman says** that one of the ways that "entrepreneurs can stay alive is by deciding to let certain fires burn so they can focus on the fires that, if allowed to rage unchecked, really will destroy the company." This wisdom can be directly applied to enterprise cybersecurity.

When surveyed, the majority of our executives identified gaps and tasks that felt daunting for security teams to take on as some of the top pain points for CISOs today. This included:

- Addressing the cybersecurity labour shortage
- Responding to the overwhelming amount of security alerts received
- Deciding what security solutions to invest in due to the crowded security solutions market

Often when it comes to enterprise cybersecurity, it can feel like there are fires all around you, and the idea of putting them all out can render even the best security team paralyzed. The solution? Figure out which fires to let burn so your team can focus on the ones that, if left allowed to rage unchecked, really will destroy your organization.

Addressing the Cybersecurity Labour Shortage

The cybersecurity labour shortage has continued to be a problem - one that's only gotten worse due to the pandemic and digital transformation that most organizations recently experienced. Drastic changes to business operations coupled with shrinking budgets have led to in-house cybersecurity professionals being difficult to come by, expensive to hire, and stretched too thin – leading to burnout and exhaustion.

While this problem can feel like a tremendous task to take on, there are digestible steps we as a cybersecurity community can take to address it. In the short term, we need to comprehensively secure organizations against their growing attack surface and the constantly evolving threat landscape. In the long term, we as a cybersecurity community need to build a capable cybersecurity workforce that will develop an industry where cybersecurity professionals can thrive, grow, and most importantly - be a part of a team that has the capacity to meet the threat landscape without being overworked, underfunded, or burning out.

Remember, there is no such thing as perfect cybersecurity. You'll never be able to put all the fires out and keep every attacker out of your system. But you can build a program that provides the best coverage and incident response to mitigate damage and provide the best ROI.

The Short-Term Cybersecurity Labour Shortage Solution

Today, in-house cybersecurity teams are tasked with a difficult challenge - catching up with business operations that have been transitioned to less secure and more complex networks with almost unbelievable speed.

Addressing this challenge requires investment in:

- Talent with comprehensive technical skills and experience
- Technology and software specific to an enterprise's unique cybersecurity needs
- Processes that enable your cybersecurity team to secure your business across all departments and employees

For many organizations, investing properly in all three in-house is simply not feasible. While we work to fill the cybersecurity labour shortage, there are many ways you can comprehensively secure your organization today:

A recent study found that the average cost saving from preventing a ransomware attack is **$396,675**.

(Deep Instinct)

Enable Your Current Cybersecurity Team

A strong cybersecurity program evolves with the dynamic risk landscape. Providing regular cybersecurity job training to keep your current cybersecurity talent up-to-date is key. Encouraging and enabling continuous learning will ensure your teamis informed on the latest trends and trained with the latest security skills.

Enabling your current program also means properly financially investing in your cybersecurity team. Ensuring your enterprise is allocating enough funding to provide the team and technological capacity to secure your organization is one of the best investments you can make. If your IT security team can't provide both cyber risk prevention and response, you are not receiving truly comprehensive coverage.

Engage a Managed Security Service Provider (MSSP)

Having the ideal mix of people, process, and technology to monitor and be ready to respond 24/7 is not always within an organization's means.

Deploying an **MSSP** as an extension of your enterprise's in-house team is a great way to supplement your existing cybersecurity program and optimize your business operations while providing:

- Access to trained security analysts and specialized experts
- A threat-centric approach that spans people, processes, and technology for faster detection and response to disrupt and block attacks 24/7/365
- Improved cybersecurity ROI from enhanced technology utilization and process optimization
- Executive metrics to measure progress and identify what risks remain within your organization in order to communicate effectively to board/executive level
- Immediate availability of hands-on incident response

The Long-Term Cybersecurity Labour Shortage Solution

There are many steps we can take to start building a cybersecurity workforce that is properly supported and invested in - and in turn, can address the growing threat landscape without being overworked and understaffed.

65% of surveyed SOC professionals reported that recent stress has caused them to consider quitting their current job.

Stop Only Considering Job Candidates That "Tick All The Boxes"

Many companies are looking for IT talent who can hit the ground running with little to no training. But **research** has shown hiring for the person first and skills second generally yields better results. The truth is that "perfect cybersecurity candidate" is often difficult to find and incredibly expensive. Many companies are missing out on some of the best employees simply because they don't have certain attributes that are easily and quickly learned.

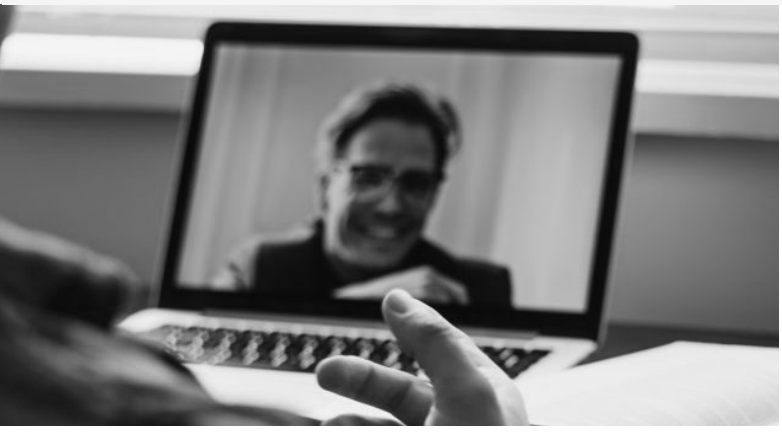
This is especially relevant for those looking to build their cybersecurity team. That candidate who is 1 year of experience short or doesn't have every preferred certification but has a great attitude and willingness to learn could be your perfect hire.

Address the Current Climate and Make Systemic Changes

Many individuals in the cybersecurity field are dealing with occupational stress and burnout. 65% of surveyed SOC professionals **reported** that recent stress has caused them to consider quitting their current job.

As we work to increase the cybersecurity workforce, it's important to address the individuals already within it. Stress and burnout happen, but we as business leaders must:

- Provide support and resources to deal with it together and in a healthy way
- Learn from the situations that have caused stress and burnout and implement meaningful change to avoid it in the future



Responding to the Overwhelming Amount of Security Alerts

Jeanne G. Harris, Co-author of Harvard Business Review's Competing on Analytics stated, "data is useless without the skills to analyze it." This may seem like an obvious notion, but all too often, we see enterprise cybersecurity programs that simply throw as many alerts as possible over the wall without the right infrastructure to enable security teams to proceed strategically. This deluge of alerts that has resulted from an increase in sophistication and frequency of cyber-attacks is unmanageable and ineffective as an approach to security. Atif Ghauri, Chief Product Officer, describes it as "a wild goose chase of alerts."

Addressing this issue requires the right skills to analyze the barrage of incoming threat data. Security teams need to build a program that can interpret and assess individual organization security requirements and leverage security insights to best prioritize their efforts and focus on direct impacts.

One of the best ways to move beyond a simple alert-based security approach is to engage a Managed Security Services Provider (MSSP) to act as an extension of your in-house security team. Unfortunately, developing a truly comprehensive in-house cybersecurity program is not feasible for most organizations. Outsourcing to an MSSP can supplement your current security program with a threat-centric approach that includes the best combination of people, process, and technology to address your specific enterprise's needs. In addition to alerting, MSSPs can provide 24/7/365 threat logging, enrichment, and escalation to drive containment and remediation efforts required to improve mean time to detection (MTTD) and mean time to response (MTTR).

Consider your in-house capabilities and existing security stack. Do you have a team with extensive cybersecurity expertise and detection and response infrastructure available **24/7/365?**

A technology agnostic, security pure-play MSSP can advise on and provide the combination of tools, technologies, procedures, and methodologies your organization truly needs to:

- Achieve real-time visibility
- Determine current detection ability
- Identify existing security gaps

When evaluating MSSPs, Adam Crawford, VP, Managed Security Services, recommends enterprises look for a provider who can:

- Increase visibility and help you better understand your risk exposure
- Work with you continuously to improve your security program
- Provide actionable intelligence
- Ensure you gain control of threats
- Help you enable your hybrid workforce
- Act as an extension of your in-house team
- Improve the ROI of your existing cybersecurity

Deciding What Security Solutions to Invest In

The security solutions market is crowded and difficult to sift through. With the increase in publicity surrounding cybersecurity, many infosec professionals have seen what Craig Jett describes as the enterprise cybersecurity solutions "drunken sailor spend". Craig explains that "many security teams are buying the newest, flashiest solutions, expecting to implement the tool and be fully secured. They do this without understanding their current security program maturity or making any necessary changes to the people or processes within their organization to make that security control work effectively. If you don't have a solid foundation set with comprehensive Identity & Access Management or e-mail phishing, there's no use implementing tools that are frankly too mature for your security program." He suggests focusing on identifying andunderstanding your current security posture and building up from there.

First you need to identify and understand the threats and risks most pertinent to your enterprise. Threat modeling against the MITRE ATT&CK Framework is a great way to achieve this. Implementing threat modelling enables your team to understand your current detection ability, the available detections that are not currently logging in your system, and any other existing gaps, in comparison to the prioritized threats your enterprise is facing.

Our Threat Modelling Approach includes:

- Identifying current security program capabilities
- Revealing gaps in coverage and ingestion based on MITRE ATT&CK Framework
- Developing a strategic tool & risk-based process plan
- Updating and improving enterprise capabilities on a regular basis moving forward

Next, quantify your organization's top risks. Craig explains, "This is so important because it allows you to put actual dollar values against your biggest risks and tell you how big of an impact that specific risk would carry should it be breached. It's about answering the questions 'if I don't do this, what might occur? What's my worst-case scenario?' This will allow you to start prioritizing cybersecurity projects and tools within your program and strategy, while also building a business case for these cybersecurity investments."

He recommends leveraging the Factor Analysis of Information Risk (FAIR) Model, an industry recognized Value at Risk (VaR) model. **The FAIR Institute** defines the FAIR Model as "a practical framework for understanding, measuring and analyzing information risk, and ultimately, for enabling well-informed decision making." The model deconstructs risks to evaluate factors that contribute to them and analyze how these factors impact each other while defining the risk in a business context.

"While the FAIR Model can be complex and overwhelming in its nature, I recommend taking a simplified approach that results in guideposts that offer a clear direction for you to go in with your cybersecurity strategy."

The best way to put a dollar value to your enterprise's top risks is to run simulations on them. Craig suggests leveraging probability analysis through Monte Carlo simulations.

This approach can identify the following about simulated risk breaches:

- The likelihood
- The timeframe
- The dollar value

Once you understand and have quantified your enterprise's specific threat landscape and risks, you can make data-driven and well-informed decisions about the security tools and solutions you invest in.

Taking a Security-Oriented Approach to Your Business

In the past, cybersecurity has been largely overlooked by executive teams and organization boards. The general outlook was that it was a purely IT and technical responsibility.

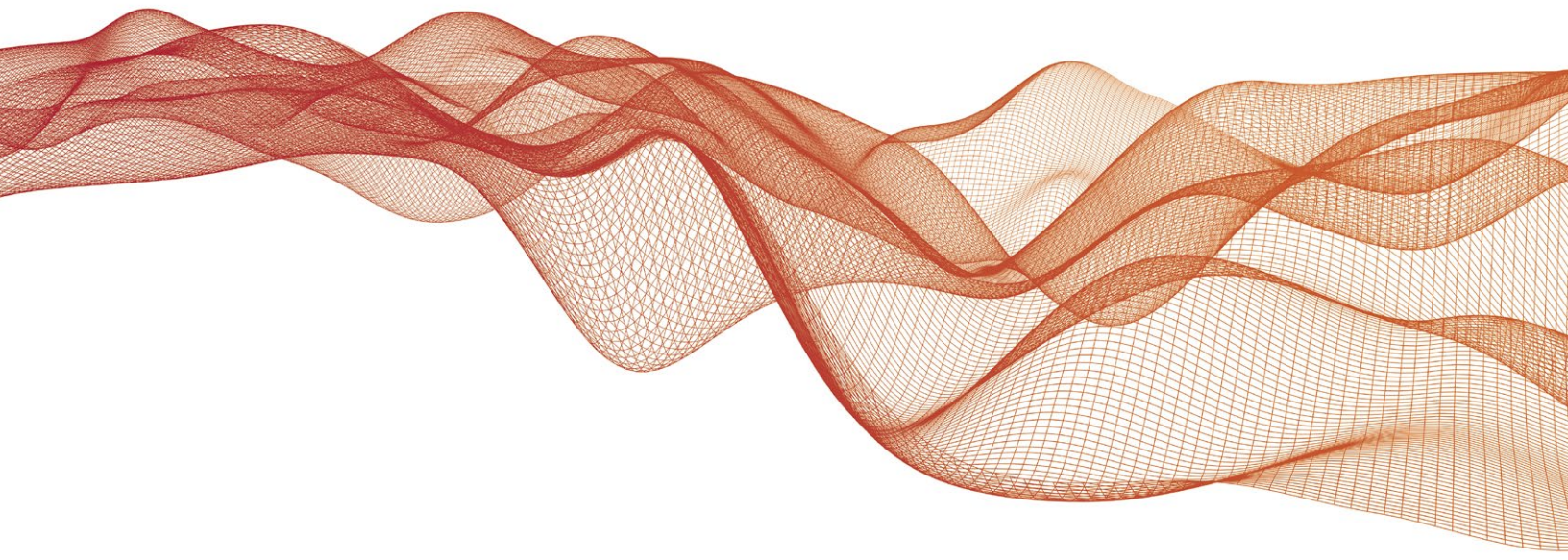
The good news – things are changing. We as an infosec community now know that, a strong cybersecurity posture is one of the greatest business-enabling tools an organization can have in its arsenal.

The bad news – there is still work to be done when it comes to changing attitudes around prioritizing information security. It can still be difficult to get executive and board-level buy-in.

It's impossible to deny the value of cybersecurity for businesses, but many security teams are still having to fight tooth and nail to convince their less technical peers and leaders that cybersecurity is a business driver rather than a cost centre.

The most successful, efficient, and cost effective cybersecurity programs are built into the very fabric of the organizations they protect. This means that the business's operations, systems, and processes are secure by design, rather than added as an afterthought. We call this taking a security-oriented approach to your business strategies.

For many security teams, implementing this from scratch is not an option. But there are many ways you can encourage security-driven approaches to your organization well after their operations, systems, and processes have been developed.



Know Your Audience and Speak Their Language

Conveying the value of cybersecurity investments to people with little to no technical knowledge is difficult and complex. One of the most difficult questions cyber professionals receive from their leadership teams is: "What will the return on this investment be?" The most effective way to answer is to quantify your enterprise's cyber risk based on given budgets and define a clear return on investment (ROI). Leverage the FAIR Model approach outlined on page 13 to quantify what your organization stands to lose as the result of not making that critical investment. Also consider explaining what it would cost in employee time, and reputational damage if you were breached.

Set expectations for your executive team and board by:

- Defining the level of protection that can be assured by varying investments in cybersecurity
- Identifying the price your business would pay if it were successfully breached
- Explaining how a cyber-attack would negatively affect critical business operations and bottom-line profits

Taking a Collaborative Approach

Cybersecurity is everyone's responsibility. Full stop. Gone are the days where defending your enterprise and knowing how to properly respond to an incident were on your IT and cybersecurity department's shoulders alone. Every person in your organization can either be your cybersecurity program's weakest link or its strongest first line of defense. To achieve the latter, ensure everyone on your team knows to be wary of suspicious activity from potentially malicious software and how to address breaches immediately when they occur.

Set up simple, accessible policies and infrastructure across all departments that support your company's employees in prioritizing cybersecurity and practicing good security hygiene including:

- Identifying and properly responding to potentially malicious activity like phishing emails that could lead to ransomware infections
- Not using easy to decrypt passwords or the same password for multiple accounts
- Keeping all device software updated

Budget Efficiently for Cybersecurity

There is no one-size-fits-all budget for enterprise cybersecurity, but there are best practices and considerations that can ensure you cover all your bases and maximize your investment while budgeting.

Assess Your Current Program First

Assessing your current security capabilities is a great place to start when building your cybersecurity budget. Understand how your current budget is being allocated. Evaluate your current program's efficacy and identify its gaps. **Ask yourself: What needs to be improved upon? What can remain the same?**

Invest Wisely

Oftentimes, leadership teams expect their cybersecurity program to cover all areas of risk. In reality, this approach can dilute the protection that high-priority areas should be getting and waste precious budget. Instead, take a data-driven approach to demonstrate an effective and tactical cybersecurity strategy. Balance spend against potential risk outcomes.

Check Compliance

Determine if your organization is required to be in compliance with any regulatory authorities. Ensure your budget covers whatever tools and practices are mandated by compliance regulations.

Don't Forget New and Potential Initiatives

When developing new business initiatives, it's important to assess and apply the appropriate security budget to ensure the initiative is properly secured. This can include engaging third-party vendors or even purchasing a team license to a cloud storage platform.

Identify Clear KPI's and Measurable Metrics

Develop clear, measurable KPIs and metrics to provide concise evidence of your cybersecurity budget's effectiveness. This will help inform future budgets and communicate the value of your program to your leadership team and board.

Ask the Experts: If I Had 1 More Dollar to Spend on Security in 2022...

Atif Ghauri

Chief Product Officer

"Security patching. It's low hanging fruit, but one of the hardest and most tedious problems to solve."

Craig Jett

SVP, Global Professional Services and Consulting

"Assessing my current security posture and identifying how to improve upon it. I'd want to know where I am today, where my vulnerabilities are, what my risks are, and what I need to do to cover those high-risk areas."

Todd Musselman

SVP, IAM

"Privileged Access Management. It is one of the least expensive tools you can implement but it has incredibly high returns on investment as it addresses the most risk."

Amiel DeGuzman

VP, Office of the CISO

"Security awareness - making sure your team is educated on the risk and security issues. This means investing in people whether it's having a more robust awareness program or investing in my infosec team and making sure they are getting the right training and resources to be more proactive in dealing with security incidents. You can have the greatest tools in the world to protect your environment but if your team doesn't know how to use it, what good is it?"

Adam Crawford

VP, Managed Security Services

"Identifying my current enterprise security posture and maturity. I would invest in strategic security services that could tell me where my gaps, vulnerabilities, and strengths are and answer the questions - am I secure? How am I measuring my security? Where do I need to improve my security program?"

Eric Dowsland

VP, Customer Success

"Vulnerability Management Whether I spend on a service organization to help mature my program, better products to automate the process, or hire dedicated bodies to help execute my remediation and patching strategy – that is where my money will go. Why? If I know there are vulnerabilities that exist in my environment but choose to do nothing about, it's tough for anyone to feel bad for me when I lose my job as a cybersecurity professional."

Chris Vermilya

Director, IAM

"Risk based multi-factor authentication (MFA). Most organizations already have basic access management in place but don't take the time to configure the risk-based access policies. Modern platforms provide many levels and configuration options to better secure the enterprise while keeping the user experience positive, use them!"

Jason Sloderbeck

Director, Worldwide Channels

"Finding the right Managed Security Services Provider. It's no longer feasible to do everything in-house and selecting the right partner to outsource MSS is perhaps the most important decision an organization will make."

Chuck Crawford

Chief Strategy Officer

"Reviewing my Identity and Access Management strategy. Border firewalls are basically a thing of the past. It's all about the user or device now. A comprehensive IAM strategy will involve compliance and data governance, and will be based off of risk with the appropriate security applied."

Executive Summary

Since the pandemic began, organizations around the world have experienced rapid mass digital transformation leaving security teams with no choice but to take a reactive approach to cybersecurity. While this approach helped us get by in these unprecedented times, it has led to:

- Team burnout
- Wasted investments
- Isolated security programs that don't cover the entire enterprise

These reactive cybersecurity strategies are unable to comprehensively secure organizations against the growing frequency and sophistication of today's threats and are not sustainable in the long term.

If we have learned anything in the past two years, it's that waiting for things to return to normal simply isn't feasible – because they likely never will. Adjusting your cybersecurity program to include proactive solutions and leverage security-driven tools within your business operations will result in a resilient enterprise cybersecurity program that can rapidly pivot and adapt to the evolving threat landscape.

To build cyber resiliency within your enterprise security program:

Embrace the constant change by prioritizing agility, visibility, and preparedness as detailed on **page 5**. Your enterprise security team will be better equipped to face the changes and demands we expect to see this year with a mix of:

- Continuous improvement **(page 6)**
- Robust identity & access management **(page 9)**
- Incident response strategies **(page 14)**

Invest wisely in your cybersecurity program by taking a data-driven approach to choosing security solutions as discussed on **page 16**. Leveraging resources like managed security solutions providers (MSSPs) can help you identify what risks, vulnerabilities, and tools your specific organization should prioritize and address daunting challenges like:

- The cybersecurity skills shortage **(page 16)**
- The continuous barrage of raw alerts **(page 18)**
- The crowded solutions market **(page 19)**

Take a security-oriented approach to your business operations by developing or adjusting your systems and processes to be secure by design, rather than as a secondary add-on as explored on **page 21**. The most successful, efficient, and cost-effective security programs:

- Properly convey the value of cybersecurity investments with clear, measurable metrics that can be appropriately communicated to all necessary stakeholders including executive teams and board members **(page 22)**
- Take a collaborative approach to integrating cybersecurity into all departments across the organization to ensure everyone that has access to your company network prioritizes cybersecurity **(page 22)**
- Implement best practices and key considerations when budgeting for your cybersecurity program to maximize your investment and optimize your solutions **(page 23)**

The time to start building a long-term, sustainable cybersecurity strategy is now. Today's threat landscape demands the ability to rapidly pivot and respond, a keen awareness of your current security posture and maturity, and above all, resiliency. Learn more about what you and your team can do to face the cyber threats and challenges in 2022 and beyond in the 2022 Cybersecurity Conversations for the C-suite Report: Cyber Resiliency for the Evolving Threat Landscape.