Research Insights

The new era of cloud security

Use trust networks to strengthen cyber resilience

IBM **Institute for Business Value**

IBM

How IBM can help

IBM Security can help you confidently move to hybrid multicloud and integrate security into every phase of your cloud journey. For more information, please visit: ibm.com/security/cloud

By Dr. Shue-Jane Thompson, Shamla Naidoo, Shawn DSouza, and Gerald Parham

Key takeaways

Executives recognize new risks and new operational demands

Scaling legacy security models exacerbates existing capacity, talent, and budget constraints. Only 35% of CISOs and 19% of CEOs agree their organization readily attracts and retains the security talent necessary to maintain an effective security posture. 49% of executives cited complexity as the greatest impediment to their security organization's effectiveness.

Cloud requires a paradigm shift in our approach to security

Cloud security operations are built for speed, scale, interoperability, automation, and collaboration. Organizations furthest along their cloud security journeys use automated solutions 6x more than those just beginning. These same organizations perform twice as well across the threat remediation lifecycle.

Security shifts from a cost center to a value driver

Across the C-suite, more than 80% of executives consider security a brand attribute that differentiates their organization. Organizations with the most mature cloud security practices outperform peers by more than 2x in terms of both revenue growth and profitability.

—

A clarion call

Most executives would agree that cloud security is important. But how important?

On December 17, 2020, the US Cybersecurity and Infrastructure Security Agency (CISA) issued the following ominous warning about the threat caused by the organized attack through the SolarWinds Orion software: "CISA has determined that this threat poses a grave risk to the Federal Government and state, local, tribal, and territorial governments, as well as critical infrastructure entities and other private sector organizations."[1]

Over the following weeks, investigators determined nation state threat actors had inserted the SUNSPOT malware into SolarWinds' Orion software updates, creating a backdoor exploit known as SUNBURST.[2] This technique compromised the integrity of SolarWinds' software supply chain, which inadvertently distributed the malware to tens of thousands of government and private entities as part of routine software updates.

The threat actors subsequently gained privileged access and used this to create backdoors into other systems.[3] While the full scope of impact may not be known for months or even years, this incident highlights a vulnerability at the heart of the cloud ecosystem: our collective reliance upon a vast network of third-party suppliers, with limited visibility into the security posture of critical providers.[4]

"It's as if you wake up one morning and suddenly realize that a burglar has been going in and out of your house for the last 6 months," said Glenn Gerstell, who was the National Security Agency's general counsel from 2015 to 2020.[5]

While this hack exposed critical vulnerabilities in software supply chain and cloud ecosystems, it also revealed the need for organizations to work together to protect each other, to form secure communities and resilient networks built upon operational and transactional trust. More than ever, security is becoming a team sport with responsibilities shared across multiple parties. Indeed, this hack came to light only as a result of coordinated investigations across impacted firms, providers, and government agencies.

81%

Across the C-suite, **81%** of executives consider security a brand attribute that differentiates their organization.

$94M

gap between CISOs and CEOs in perceptions of their organization's total annual risk exposure.

more than 2x

Organizations with the most mature cloud security practices outperform peers by **more than 2x** in terms of both revenue growth and profitability.

The cloud security conundrum

As cloud ecosystems mature, it is becoming evident that the same platforms, technologies, and services that make the cloud so powerful can also become a source of vulnerability. A growing concern among security leaders: how do we make sure our investments in cloud are working for us?

A June 2020 IBM Institute for Business Value (IBV) study found that nearly 90% of cloud spend is devoted to either public or hybrid clouds, and 40% of overall workloads operate across multiple clouds.[6] Our approach to security operations must adapt to these new ways of working, where perimeters and trust are negotiated in real time. With the pandemic and SolarWinds at top of mind, leaders need to recognize that every cloud conversation must also be a security conversation.

This report explores how cloud infrastructure, technologies, and services are transforming cybersecurity operations. We asked 930 security and business leaders from 17 industries and 20 countries to assess their cloud operations from two perspectives (see Research methodology on page 21). First, how rapidly are their organizations migrating business operations to cloud and, second, what is the relative maturity of their cloud security operations? We used this data to better understand if cloud security capabilities are keeping up with cloud migration.

This report's chapters present our findings from three perspectives:

- Understanding risks
- Shifting the security paradigm
- Re-envisioning security to drive value.

COVID-19 has accelerated long-standing trends while also making investments in digital transformation more urgent.

Chapter 1: New capabilities, new risks

Cloud migration can expose new vulnerabilities and attack vectors

As the world of work is transformed by the pandemic, leaders are assessing operations and new ways of running their businesses. COVID-19 has accelerated long-standing trends while also making investments in digital transformation more urgent.

The rapid and unexpected shift to remote work models highlights the benefits of decentralized cloud infrastructure and cloud security operations. For example, at the outset of the crisis, many organizations ramped up their use of multi-factor authentication, zero-trust security frameworks, and security policies designed for flexible work environments.

But the transition to cloud operating models has also highlighted fundamental dependencies and limitations—and the resultant risks—at the core of digital supply chains and digital operations. Operational constraints, *ad hoc* remote-work arrangements, and an unexpected mix of devices and access points have exposed organizations to new risks.[7]

For the purposes of this study, we have defined five stages of cloud security transformation (see Figure 1):

- *Evaluating.* Early-stage cloud security operations encompassing pilot projects and/or limited production deployments. Identifying candidate use cases, formulating business strategy, and/or building a value case for cloud security.
- *Investing.* Deployment(s) of cloud security underway with value being realized. Strategy and business cases are in place.
- *Integrating.* Infrastructure and processes support the secure flow of data between various cloud and on-premises environments that support business functions. New cloud-based offerings/services are securely enabled.
- *Optimizing.* Taking full advantage of data flowing securely between multiple cloud and on-premises environments. Cloud security functionality and benefits are realized.
- *Innovating.* Capability exists to securely enable and extend new cloud-native business and operational opportunities to internal and external partners. Operational feedback drives perpetual improvements.

While cloud adoption is undoubtedly driven by business objectives, security concerns and considerations play a fundamental role in cloud transformation efforts. For most organizations, cloud security is still a work-in-progress.[8] A 2020 IBV study found that only 42% of respondents report they have multicloud security and compliance deployed across their entire IT infrastructure.[9]

Figure 1

Transformation stages

First, build strategy and business case, then drive ROI as capabilities mature

Security operations teams can achieve breakthrough results when strategy, design, and governance reinforce each other.

For the present study, executives surveyed indicated their cloud risk exposure increases as cloud footprints expand (see Figure 2), but also that security postures can improve as organizations enhance their cloud security maturity (see Figure 3).

These findings suggest that investments in cloud security are paying off, but also that modernizing operational and governance practices is essential to maintaining an effective security posture.

Complexity is challenging security organizations

Forty-nine percent of executives surveyed cited complexity of infrastructure or operations as their most critical challenge. This is by far the leading impediment to the security organization's effectiveness, cited nearly twice as often as the next leading factor.

Of note, many of the other factors cited—such as lack of talent (22%), governance concerns (22%), lack of skills (20%), and lack of operational alignment (20%)—may also reflect underlying issues related to complexity.

More than one-third of all organizations have purchased 30 or more cloud services from 16 different providers, according to a 2019 study by IDC.[10] And a recent Forrester study found complexity erodes ROI and inhibits innovation, while addressing complexity makes organizations more resilient.[11]

Security governance—whether in the form of security standards, administrative policies or control frameworks—is first and foremost a design consideration. What differentiates high performance security operations teams are the innovative ways they mitigate complexity to improve efficiency, consistency, and quality.

Figure 2

Risks by stage

As more operations move to the cloud, the percentage of security incidents that are cloud-related also increases

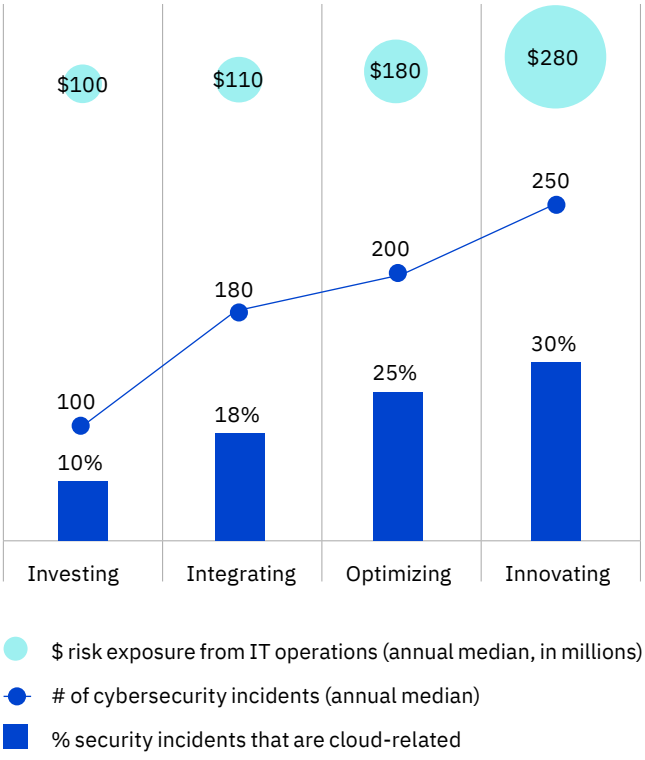
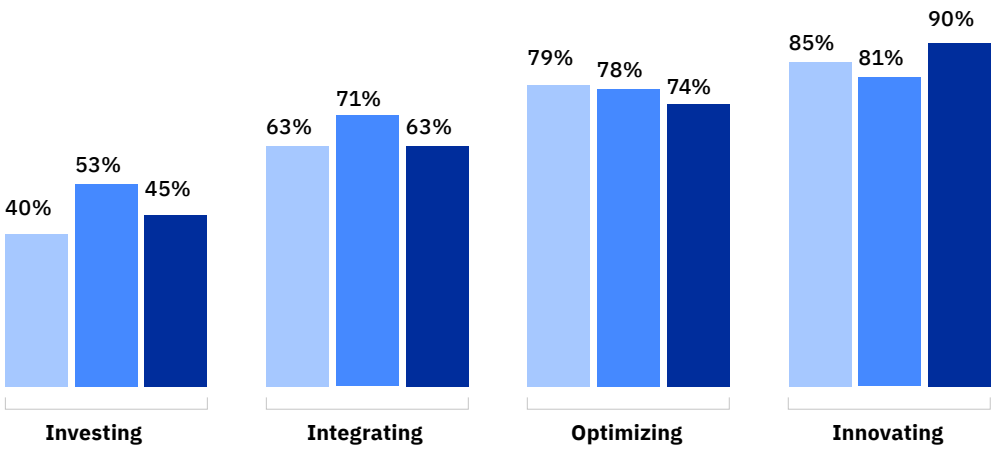


Figure 3

Security dividends

Security postures improve as organizations enhance their cloud security capabilities



Our cloud operations are consistent with our security posture
We maintain a consistent security posture across our cloud providers
We maintain real-time visibility into security events and how they impact our overall security posture

Security operations teams can achieve breakthrough results when factors of strategy, design, and governance reinforce each other. In our sample, this holistic approach to security operations is best represented by a sub-group we call "Cloud Security Bellwethers."

Respondents from the Bellwether sub-group indicated they outperform peers more than 2x in terms of both revenue growth (86% versus 40%) and profitability (84% versus 38%). See "Perspective: Cloud Security Bellwethers shift the security paradigm."

Perspective: Cloud Security Bellwethers shift the security paradigm

Organizations in the early stages of cloud migration and security evolution can learn from those that have already made significant investments in their cloud security operations. In our sample, 28% of organizations—Cloud Security Bellwethers—stand well apart from peers, in terms of security performance, technical proficiency, operational agility, and cloud security maturity (see Figure 4).

Bellwethers integrate their cloud and security strategies to a greater degree than others, in large part because they're preparing for a hybrid, multicloud world. These organizations are optimized for cloud-native operations, designed for partner integration and collaboration, and promote resilience through the adoption of leading practices and common governance.

Because they have worked through many early-stage integration challenges, Bellwethers can serve as guides for how to implement a comprehensive cloud security program.

As they gain greater maturity, Bellwethers are finding ways to improve their overall security posture with cloud-centric security capabilities. They have developed cloud-native security operating models centered on shared responsibility, agile security operations, and streamlined security governance.

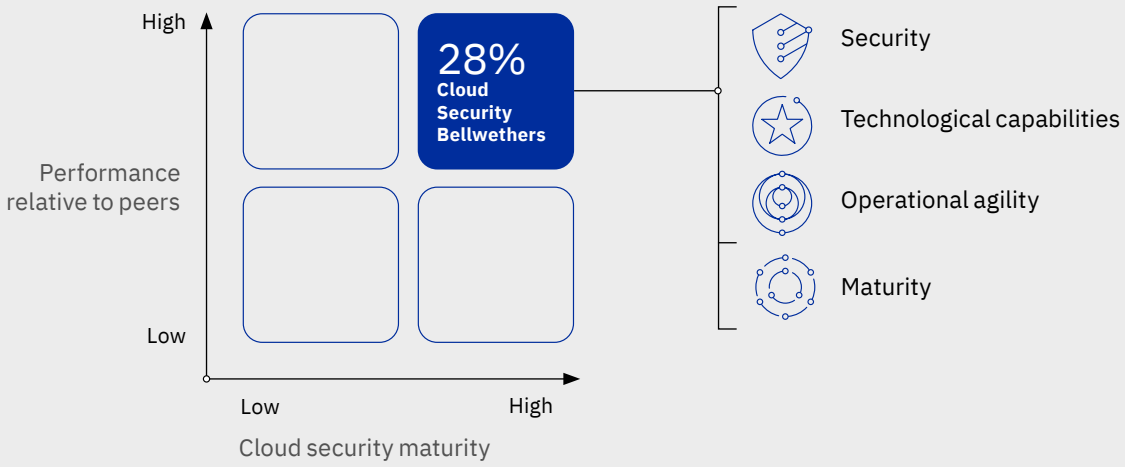
These capabilities help Bellwethers help Bellwethers draw insights from data and collaborate more effectively with partners. They also open the door to new value propositions across the broader cyber portfolio.

Bellwethers stand apart from other organizations in four significant ways (see page 7).

Figure 4

Standing out

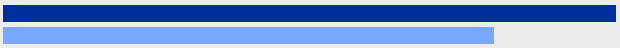
Bellwethers make up 28% of respondents and rank themselves highly on 4 factors



Bellwethers | **All others**

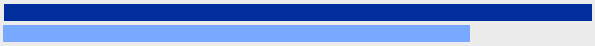
They connect cyber risk, security, and resilience to their organization's core mission

96% | 77%



Bellwethers influence organizational strategy at the board level

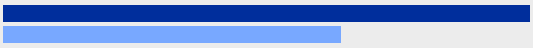
92% | 74%



Bellwethers' security operations teams have clearly defined success criteria.

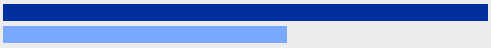
They automate for quality, scale, and specialization

83% | 53%



Bellwethers use automation to respond to security events

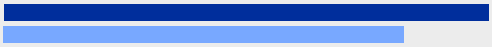
76% | 45%



Bellwethers rely on machine learning and AI to enhance their security operations

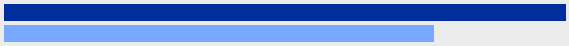
They prioritize operational agility to generate insights

76% | 63%



Bellwethers routinely incorporate security telemetry into their data analysis

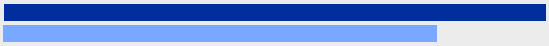
88% | 67%



Bellwethers have enhanced their security posture by simplifying and standardizing their technology toolsets

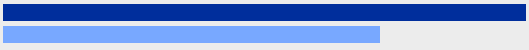
They integrate security operations with partners

85% | 68%



Bellwethers maintain a consistent security posture across cloud providers

82% | 59%



Bellwethers maintain visibility into their partners' supply chains

When security becomes a design consideration, the downstream complexity of IT infrastructure and operations is reduced.

A new approach: shifting security left

Making security functions an integral, consistent part of product and service design—rather than treating security requirements as an afterthought—is sometimes referred to as "shifting security left." When security becomes a design consideration—a way of doing business more securely and more transparently—we reduce the downstream complexity of IT infrastructure and operations.

Similarly, cloud-native operating models like DevOps and DevSecOps are gaining in popularity because they address development, configuration, and support in a holistic manner, as interdependent variables (see Figure 5). DevOps consolidates software development, deployment, and support functions to enable continuous integration and delivery (CI/CD) capabilities. DevSecOps is a refinement of DevOps where security capabilities are incorporated into the development and delivery lifecycles.

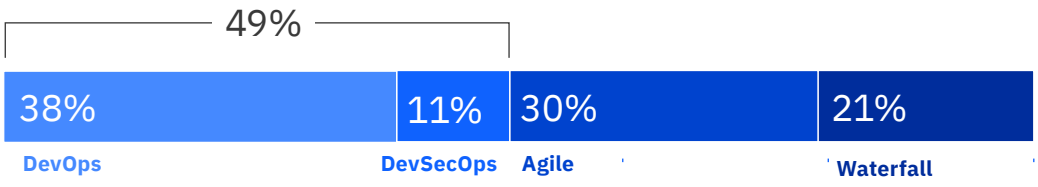
Zero-trust security models extend the security umbrella even further by explicitly transforming trust into an operational variable—using access controls, contextual data, and risk/trust scoring to deter non-moderated movement inside the network. When integrated with identity management solutions, zero-trust designs can create personalized, yet highly secure, interactions.

However, we must remember new applications, services, or operational capabilities do not afford better security in and of themselves; if anything, they can introduce new risk and make the security environment more complex. Migration to cloud security application platforms will have little impact unless security operations and governance practices are also modernized. Of course, this is easier said than done. One of the biggest challenges facing CISOs today is balancing business imperatives with security operations concerns.

Figure 5

Security first

49% of respondents now use DevOps and DevSecOps to integrate security capabilities into IT infrastructure and operations



Leadership strategies and priorities diverge

Even organizations that say they are most mature in their cloud security practices are not always able to maintain a consistent security posture. Among the most mature organizations (those in the "Optimizing" and "Innovating" stages), nearly 1 in 5 did not agree or were ambivalent about whether their cloud operations were consistent with their organization's security posture. More than 1 in 5 did not agree or were ambivalent about whether they maintain a consistent security posture across cloud providers.

Among executives, we found inconsistent views of security operations across the organization. At first glance, leaders' views of their technology and security strategies seem aligned: 91% of CISOs indicated their cloud and security strategies are tightly coupled, while 80% of CEOs agreed. Yet under the surface, cracks emerge.

Three-quarters of CISOs reported their cloud operations were consistent with their security posture, while only 62% of CEOs concurred. Similarly, markedly fewer CEOs expressed confidence in their cloud security roadmaps (69%) compared to CISOs (92%). Even though CISOs and CEOs report their cloud and security strategies are in sync, the above findings suggest important gaps exist.

For organizations in the midst of cloud transformation—which is to say, *most* organizations—these differences in perspective can have a profound influence on ongoing security modernization efforts.

Compared to CEOs, CISOs calculate the cost of breaches as 40% higher ($3.6 million versus $2.6 million per breach), and they report 20% more breaches per year (65 versus 54). These differences amount to an eye-opening $94 million discrepancy in total annual risk exposure.

This raises questions: what is causing this discrepancy, and what are the operational implications for any disconnect between security operations and business strategy? If it is true many CEOs are underestimating both the frequency and magnitude of their IT risk exposure, this may be influencing administrative decisions in critical areas beyond risk management, such as security budgeting and staffing.

Moreover, though differences in perception are understandable given executives' varied responsibilities, often these differences lead to divergent priorities that are reflected in *ad hoc* security decision-making, conflicting views on budget requirements, or a lack of board visibility and accountability.

Most importantly, executive misalignment means core concerns and root causes are often the last and most difficult to address—a consequence that can have profound impacts on the organization's overall security posture.

These insights suggest security and business leaders should engage in deeper conversations about risk and value. When cloud and security innovations are deployed in tandem, risk is reduced, new value propositions emerge, and business resilience is enhanced. See sidebar, "Ford Motor Company: Modernizing for innovation, speed, and resilience."

Chapter 2:
Rethinking security operations

Security business-as-usual does not scale for cloud security operations

If cloud can create new vulnerabilities—as is often the case for organizations just beginning their cloud security journeys—then ramping up existing security operations practices may make current resource, skill, and capacity constraints worse. That's because legacy security operations models are not designed for cloud-native variables—namely speed, scale, interoperability, automation, a changing mix of services, and shared responsibility for security outcomes with partners outside the organization (see Figure 6). Any one of these variables puts new pressures on security operations. Cloud is built on all these variables working together, simultaneously.

In cloud operations, traditional security practices, such as, network perimeters and privileged access, are joined by new capabilities like endpoint awareness, multi-factor authentication, real-time data/metadata analysis, and automated policy administration. This represents a profound change. From consumer experiences to business intelligence, cloud security services are becoming essential to value generation. Cloud security goes beyond securing the cloud; it is a core part of business enablement.

Figure 6

Where legacy lags

Traditional security operations fail to take advantage of cloud-native capabilities

Traditional security operations	→	Cloud security operations
Longer planning cycles Infrequent deployment and patch schedules; security functionality added after-the-fact	→	**Agile operations** Iterative sprints, responsive decision-making, and security governance-by-design
Large, monolithic applications Complex, not easy to scale, difficult to update	→	**Open standards and interoperable services** Modular, easily upgraded APIs and microservices
Many manual processes Capacity constraints and skill shortages limit flexibility	→	**Highly automated and aware** CI/CD based on real-time insights and automated response capabilities
Siloed goals and objectives Separate development, security, and operations teams	→	**DevSecOps** Integrated operations, support, and governance to improve security outcomes
Cost center disconnected from value creation Security operates independently on fully owned and operated solutions	→	**Shared value and shared responsibility** Security is interdependent, sustained by a community of ecosystem partners

Hybrid multicloud security operations are distinguished by fluid, multi-party collaboration.

Ecosystems evolve: Re-orienting around a shared responsibility model

Perhaps the most significant change in a cloud security operating model involves new ways of working together. Traditional security operating models presume full visibility across owned and operated security platforms. Cloud security is based on a more distributed operating model, with security services federated across multiple assets, datastores, and providers.

Given the scale and speed of cloud security operations, responsive communications, mutual problem-solving, and agile decision-making are necessary for sustaining cyber resilience. This requires a new model for security governance based on shared responsibility.

Hybrid multicloud security operations are distinguished by fluid, multi-party collaboration, and interlocking agreements about who's responsible for what (see Figure 7). This encompasses a wide range of capabilities, such as managed security services, proprietary vendor insights, and specialized services—artificial intelligence (AI) and infrastructure-level services like telemetry and log capture, for example.

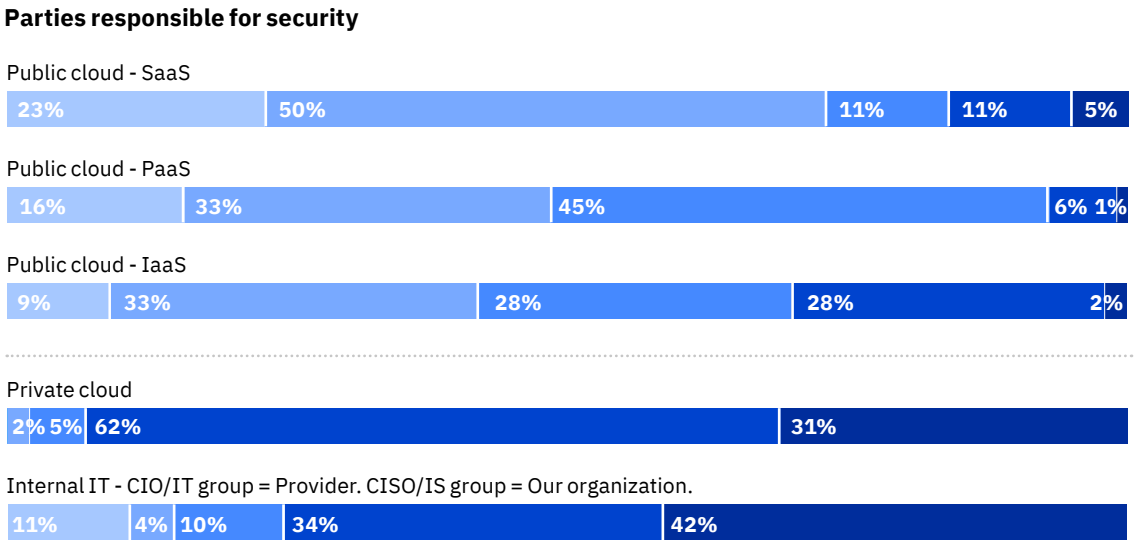
The increased availability of partners using standard design patterns highlights one of the key advantages of cloud security: by standardizing applications and infrastructure, providers can offer value-added security services as an extension of their core cloud functionality. Indeed, this study found 66% of executives are looking to their cloud providers to provide a baseline level of security.

—

Figure 7

Shared responsibility

Hybrid multicloud security operations feature fluid, multi-party collaboration



Q: How does your organization allocate responsibility for securing the following technology infrastructure?

Cloud security requires communication, collaboration, and consensus, so CISOs must place new emphasis on their people and relationship skills.

Rethinking security leadership: The role of CISO evolves

As chief proponents of the security value proposition, CISOs need to be able to articulate a security strategy consistent with the organization's broader business objectives. Most importantly, CISOs need to feel at liberty to expand the cybersecurity conversation beyond their expected vigilance regarding data breaches to a broader conversation about cyber resilience, data integrity, operational trust, and privacy. The shared responsibility models essential to cloud security mean CISOs will need to place greater emphasis on business advisory, operational insights, collaboration, and innovation.

Every organization operating multiple cloud environments —something true for most organizations today—must address how they will maintain a consistent security posture across a myriad of cloud service providers offering a diverse set of runtime environments.[12] Fully 70% of respondents indicated they need to measure, monitor, and secure workloads across multiple public and private cloud providers, while 72% said their organization needs to maintain a consistent security posture across providers.

The role of CISO needs to adapt to meet these demands. The growing reliance on third-party providers outsources some infrastructure and platform requirements. But it doesn't factor in the need to maintain a consistent security posture across a wide variety of federated services, distributed operations, and often divergent approaches to governance.[13]

Furthermore, organizations' increasing reliance on data insights and automation means today's security leaders must possess both up-to-date technical skills, as well as the people and communication skills required to run a collaborative security practice.[14]

Because security outcomes encompass a wide variety of factors, CISOs' leadership skills are becoming more important than ever. Because these outcomes are based on communication, collaboration, and consensus,CISOs must also refine their people and relationship skills to build commitment inside and outside the organization.

Rethinking the talent strategy: Enhance capacity and skills with AI and automation

By adopting the same cloud-native capabilities as the organizations they seek to compromise, today's threat actors are becoming more potent and more elusive. The proliferation of attack surfaces and the accelerated pace of business operations can challenge even the most talented security operations teams. Operational complexity elevates risk because it typically requires human judgment for remediation. As more operations move to cloud, security events multiply, yet skilled security analysts grow increasingly difficult to find and hire.

Persistent resource, skill, and capacity shortfalls can devolve into critical risk factors.[15] In our study, both CISOs and CEOs recognize resource constraints are impacting their ability to maintain a consistent security posture. Only 1 in 3 CISOs and 1 in 5 CEOs expect they can attract and retain the talent necessary to maintain an effective security posture.

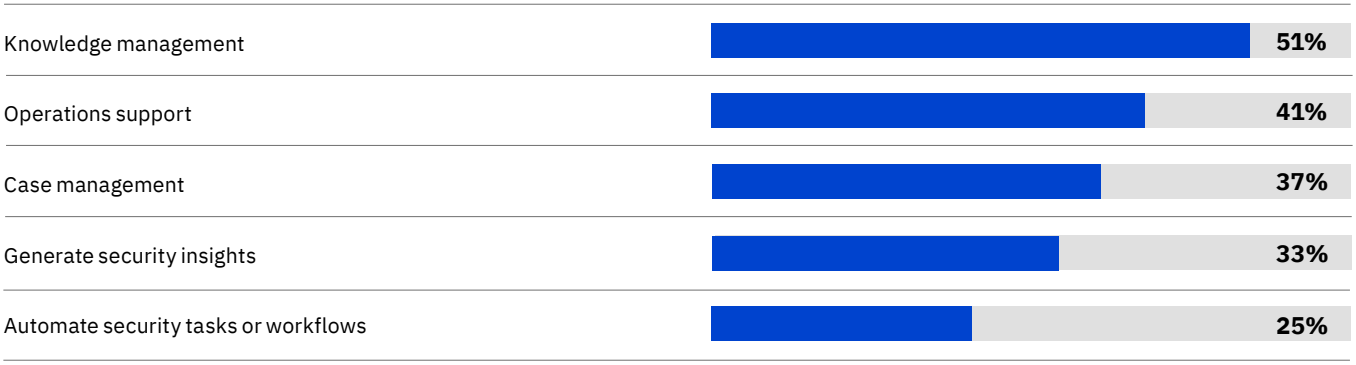
One of the more promising opportunities presented by cloud-based security is the potential for collaboration among automated services, AI-based virtual agents, and skilled human analysts. Increasingly, AI and machine learning technologies are playing a prominent role in security talent support functions, such as knowledge bases, case management, operational insights, and automation (see Figure 8). These technologies complement and extend the capabilities of skilled human analysts—either by way of curating data, reducing cognitive loads, or expediting analysis.

In practice, these tools add additional capacity to security operations teams. By offloading more routine administrative tasks, such as those associated with the exponential growth of devices and data,[16,17] leaders can focus on attracting and retaining the more specialized security operations skills that have the biggest impact on security outcomes.[18]

Figure 8

Tech supports talent

AI and machine learning technologies extend what skilled security analysts can do on their own



Q: Approximately what percentage of your security operations incorporate the following artificial intelligence (AI) and machine-learning (ML) capabilities?

The future of cloud ecosystems: Community-based security

Considering the importance of collaboration and shared responsibility, perhaps the most significant trend in security operations is the rise of cloud-based security services, which promote interoperability and orchestration across providers. Services emphasize common standards, modularity, transparency, and accountability to achieve scale and facilitate automation.

Examples include open-source libraries, crowd-sourced software development tools, and threat intelligence sharing.[19] These independent communities are critical in contributing expertise, developing new design patterns, and advocating community-based standards for security governance.

As hybrid multicloud becomes the norm, technology and security leaders need services to promote efficiency and resilience, not more complexity. Open security frameworks present an opportunity to make security less proprietary and less insular. Building a robust community is a critical first step in developing future talent, aligning efforts around common standards, and streamlining operations to promote collaboration—all of which are vital steps toward enhancing cyber resilience.

Open security frameworks combine community-validated designs with community-driven feedback and community-based support. This approach encourages participation, sharing, standardization, and simplification. In terms of security strategy, the virtue of open cloud designs is that they transform complex operational variables, including hardware, software, configuration, and support, into a series of standardized services that can be delivered and administered across different clouds and different providers.

Moreover, a community-based approach to cybersecurity makes sense because would-be adversaries have already adopted community-based approaches to threat operations. For example, cybercrime-as-a-service and illicit markets share advanced malware assets and tradecraft.[20]

The ability to add capacity, staffing support, or expertise on demand is a key selling point for cloud solution providers.

Chapter 3: The cloud security value proposition

Use investments in cloud to enhance security performance

As more workloads move to cloud, and as cloud evolves to support a broader range of workloads, organizations with the greatest commitment to cloud security are seeing a noticeable improvement in threat remediation performance.

The most mature organizations perform twice as well as the least mature, with a cumulative mean-time-to-identify and mean-time-to-contain of 125 days versus 250 days, respectively (see Figure 9). A similar pattern is revealed when assessing automation: the most mature organizations report using security automation nearly 6x more than the least mature organizations.

One of the primary benefits of cloud ecosystem partners is that they have developed what others cannot—namely, the resources, specialization, and infrastructure necessary to operate hyperscale, cloud-native businesses. The ability to add capacity, staffing support, or expertise on demand is one of the key selling points for cloud solution providers. This applies to specialized cloud security providers, but also, more generally, to hyperscale cloud providers offering security services.

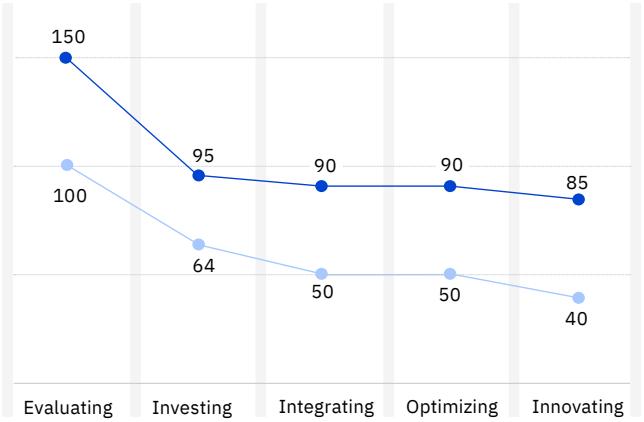
The integration of cloud infrastructure and operations offers a combination of flexibility, capacity, standardization, and specialization that is key to enhancing security performance outcomes. By working with partners, adopting common approaches to security operations and governance, and finding the right mix of build-versus-buy capabilities, organizations can maintain an effective security posture even in highly dynamic operating environments.

Figure 9

Threat remediation

With more mature cloud security in place, threats are both identified and contained significantly faster

Threat remediation KPIs by cloud security stage



Data breaches - Mean time to identify, in days
Data breaches - Mean time to contain, in days

Use investments in security to improve business outcomes

Whereas in the past, security was thought of narrowly as only "threat remediation," perceptions of security are changing. Leaders across the organization recognize security as a component of business quality. More than 80% agree security, assurance, and trust are brand attributes that differentiate their organizations. Similarly, 83% said security adds value to the organization's products and services, while 87% indicate security is integrated into their daily operations and a vital part of their organization's culture.

These views are shared by leaders inside and outside the security domain. There is a consensus across the C-suite—not just among CISOs and CIOs, but among CEOs and COOs as well—that the security value proposition is expanding, in large part due to the new capabilities enabled by cloud infrastructure and services.

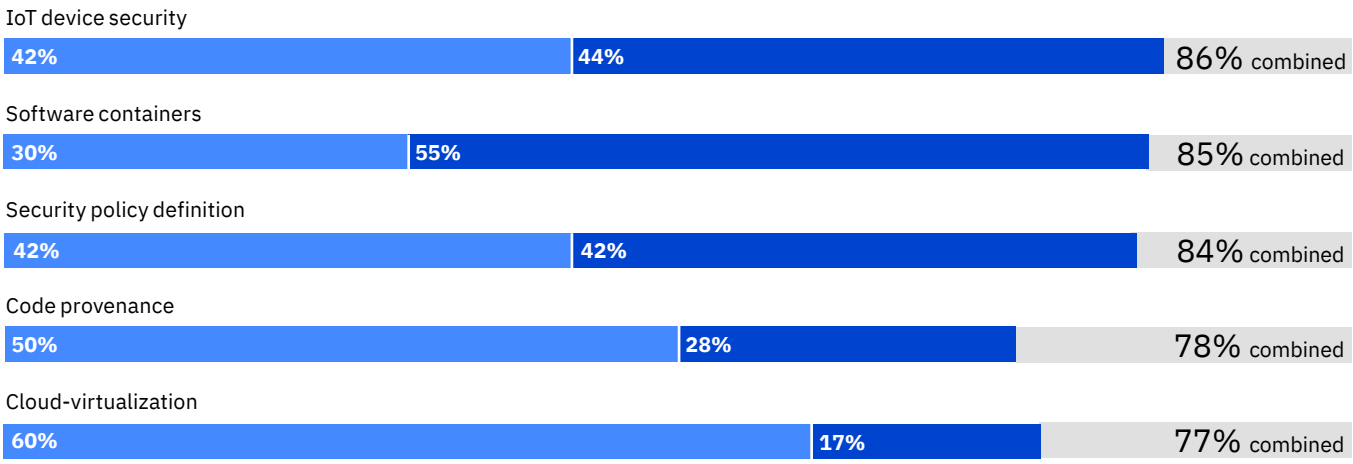
Looking ahead, cloud technologies will likely serve as the foundation for nearly every innovation in the security portfolio. Organizations are prioritizing development of capabilities for IoT device security, software containers, security policy administration, and software supply chain, among others (see Figure 10).

This makes collaboration between CISOs and their technology peers (such as CIOs, CTOs) essential. It also underscores the increasingly important role CISOs play in enabling not just security operations but, more generally, new operational capabilities and new value propositions.

Figure 10

Investing in innovation

Cloud technologies enable a host of capabilities to strengthen the security portfolio



Note: Figure shows percentage of respondents choosing answers 4 or 5. Q: What role do you anticipate each of the following capabilities will have in your organization's cloud security posture over the next two years?
1 - No role; 2 - Proof of concept/experimentation; 3 - Supporting role limited to geo or function;
4 - Organization-wide capability; 5 - Core organizational capability (differentiator)

Use collaborative security models to enhance cyber resilience

In response to an ever-expanding threat landscape, security operations are evolving from a traditional emphasis on threat mitigation to more holistic concerns like cyber resilience. Cyber resilience addresses the entire security lifecycle in a comprehensive and systematic way, as a series of interlocking capabilities designed to enhance the organization's overall security posture.

As described by Ponemon Institute, "A cyber resilient enterprise successfully aligns continuity management and disaster recovery with security operations in a holistic fashion."[21] This expanding view of the security portfolio is at the heart of the cloud security value proposition.

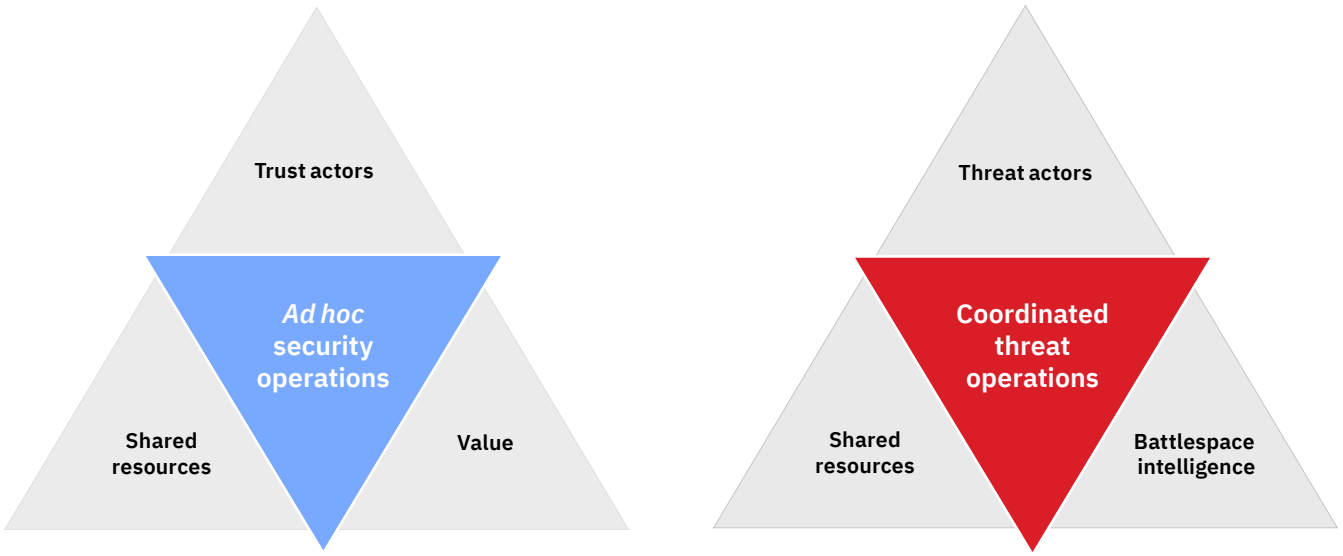
Accompanying the shift to cloud-centric operating models, data and operations are increasingly federated across partners. Threat actors are targeting strategic partners, and as a result, threat vectors are extending out from the individual organization to the shared ecosystem.

Today, cloud ecosystems are vulnerable because visibility is limited (see Figure 11). Trust actors share resources to create value. But they typically share insights or governance on an *ad hoc* basis, after the fact. Threat actors use these gaps to probe for vulnerabilities and to undermine trust. They coordinate operations and share information to maximize leverage. For trust actors, the lack of ecosystem-wide cyber awareness and response capabilities degrades cyber resilience and puts value-realization at risk.

Figure 11

Today: A cyber arms race

Threat actors exploit vulnerabilities at the ecosystem level, which requires *ad hoc* remediation across parties



By re-framing security operations as a form of community, the same dynamics that can make the organization more vulnerable can also make it more secure and resilient.

But if leaders shift their perspective to focus on the shared responsibility model, new possibilities emerge (see Figure 12). By thinking of the ecosystem as a community built on mutual investment and mutual commitment, trust actors benefit from sharing information and working together.

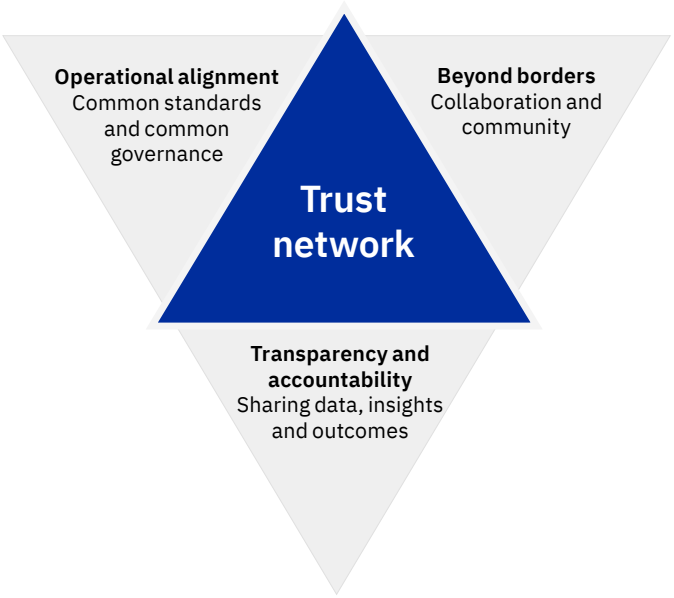
Whereas in traditional ecosystems organizational boundaries serve as break points and lack of visibility creates shared risk, in a trust network, multi-party (aka collective) security becomes the norm. Responsibility is shared across supply chain and partner networks. Over time, many approaches become one. As a result, all parties benefit from enhanced cyber awareness and cyber resilience.

—

Figure 12

Future: The trust network advantage

Greater accountability and information sharing across the ecosystem enhances cyber resilience for all parties



Just as bad actors coordinate efforts, and share information and resources on the dark web, leaders can choose to re-orient operations around transparency, accountability, and trust in order to share insights and scale operations in conjunction with their trusted network partners.

- By re-framing security operations as a form of community, the same dynamics that elevate risk and make the organization more vulnerable can also make the organization more secure and more resilient.
- By working together, complexity and fragmentation can be transformed into specialization and scale.
- And by prioritizing visibility, sharing, and common governance, leaders open the door to new value propositions that extend beyond organizational boundaries.

Finally, cloud security is essential to enabling and extending new operational capabilities that are adjacent to the cybersecurity domain. For example, cyber risk, supply chain integrity, identity management, and operational trust are practice areas that are vital to enhancing overall cyber resilience.

While the market dynamics are still evolving, the implications are clear: cybersecurity is no longer simply a cost center; it is becoming a value driver—a sentiment expressed by 83% of survey respondents.

Make every cloud conversation a security conversation

As we plan to adapt to life after COVID-19, we are likely to see our relationships and our organizations in a different light. In this new normal, cloud ecosystems will increasingly leverage community-oriented and collaborative approaches to security.

The first step is choosing to see our cloud ecosystems for what they are—trusted operating environments for trusted partners. By synthesizing cloud-native capabilities, shared investments in capacity, and collaborative security governance, cloud ecosystems are naturally evolving into trust networks. By insisting that every cloud conversation is also a security conversation, leaders can shift the conversation from security awareness to cyber resilience.

By putting strategy and design considerations first, cloud-based trust networks open the door to entirely new ways of working together and creating value. As leaders prepare for the next phase of their cloud security journeys, these are the kinds of opportunities that will differentiate one organization from the next.

Action guide

The new era of cloud security

Six principles help organizations tranform a cloud security ecosystem into a trust network.

Understand the risks

1. Adopt a unified strategy that combines cloud and security operations	– Assess how security strategy serves (or doesn't serve) as an extension of organizational strategy. – Make sure CxO leaders share a similar perspective on vulnerability and risk.
2. Modernize security operations in line with cloud investments	– Objectively assess cloud risk exposure using standardized measures, preferably measures that align with partners. – Streamline operations to remove friction and complexity.
3. Re-envision security for shared responsibility and outcomes	– See risk holistically across internal and external boundaries. – Use a common governance framework to standardize risk classification, communications, and threat remediation capabilities with your ecosystem partners.
4. Leverage smart technologies to meet the demands of cloud security operations	– Assess the impact of cloud-native variables like scale, speed, interoperability, automation, a changing mix of internal and external services, and shared responsibility. – Document the cloud and security factors unique to your organization that influence your risk profile and security posture.
5. Redefine the cybersecurity value proposition by focusing on business resilience	– Use risk modeling and risk quantification to understand the impacts and probabilities associated with various operations scenarios (such as vendor or supply chain compromise). – Estimate the financial costs of maintaining cyber resilience and business continuity prior to an incident, during an incident, and after an incident.
6. Think of security as a community, and use this to enhance trust	– Develop measures for monitoring and improving security collaboration, shared responsibility, and collective resilience across the ecosystem. – Transform security awareness into a cultural concern that extends across and beyond organizational boundaries.

Shift the security paradigm

1. Adopt a unified strategy that combines cloud and security operations	– Develop your cloud security strategy by assessing opportunity and risk at the organizational level. – Formalize a unified cloud and security roadmap that ties together organizational objectives, cloud operational capabilities, the organization's risk profile and desired security posture.
2. Modernize security operations in line with cloud investments	– Consolidate platforms and standardize offerings to promote internal and external collaboration. – Integrate security into the operations and support lifecycles (DevSecOps).
3. Re-envision security for shared responsibility and outcomes	– Think creatively about how to make governance practices easy to adopt. – Automate security policy administration and security control frameworks. – Investigate supply chain attack vectors and reduce attack surfaces by increasing visibility, sharing information and pooling specialized resources.

4. Leverage smart technologies to meet the demands of cloud security operations	– Re-orient security operations around the ability to generate and act upon insights (such as telemetry data, analytics, forensics, threat intelligence services). – Use AI and automation to empower analysts, gain deeper insights, and improve security outcomes.
5. Redefine the cybersecurity value proposition by focusing on business resilience	– Brainstorm how security operations might benefit from open, cooperative, and community-based security frameworks. – Develop a more collaborative security operating model optimized for shared services across multiple cloud partners. – Adopt common governance frameworks, standardize risk and threat classification schemas, and align operational practices to extend security capabilities beyond organizational boundaries.
6. Think of security as a community, and use this to enhance trust	– Integrate internal and external partners into security simulations. Drill for complex scenarios including zero-day exploits, ransomware, and advanced persistent threats. – Create an ecosystem-wide security operations center (SOC) with a coordinated incident management/crisis response capability.

Re-envision security to drive value

1. Adopt a unified strategy that combines cloud and security operations	– Articulate how security serves core brand values and emphasize the role of resilience in protecting brand capital. – Demonstrate how security operations and security-adjacent operations serve colleagues' business objectives and business outcomes.
2. Modernize security operations in line with cloud investments	– Standardize your investment criteria and thresholds for returns, then choose where to specialize and where to generalize. – Embrace open security solutions that work across cloud providers.
3. Re-envision security for shared responsibility and outcomes	– Make security awareness and information sharing cultural norms ("Security is a team sport"). – Invest in talent and partner relationships that help your organization scale and differentiate.
4. Leverage smart technologies to meet the demands of cloud security operations	– Make security perspectives an integral part of strategic planning, product development, and innovation efforts ("shift left"). – Remove friction by making security controls automatic (zero-trust). – Learn from others. Consider the ways peer organizations have developed and refined their cloud security capabilities over time.
5. Redefine the cybersecurity value proposition by focusing on business resilience	– Document how cybersecurity contributes to value-generation—for example, as an anchor for multi-party security operations, as a vehicle for new ways of working with internal and external partners, or as a channel for reinforcing brand values of integrity, transparency, and trust. – Explore the ways your cloud ecosystem is already functioning as a trust network.
6. Think of security as a community, and use this to enhance trust	– Assess the ways talent, skill, and capacity gaps can be re-framed as opportunities for co-creation, collaboration, and specialization. – Leverage the breadth and depth of ecosystem partners by sharing resources, expertise, and information. – Choose open security solutions to optimize talent pools, interoperability, and scalability.

About the authors

Dr. Shue-Jane Thompson
linkedin.com/in/shuejane
shuejane@us.ibm.com

Dr. Shue-Jane Thompson is the Vice President and Sr. Partner for Security Strategy and Growth Service Line at IBM Global Business Services Sector. She oversees cybersecurity solution innovation, integration, services sales and delivery for clients across 170+ countries worldwide. Dr. Thompson has more than 30+ years of experience in academia, commercial, government and international technology and business management environments, including winning and managing many large-scale IT, cyber, cloud and mission-operation programs.

Shamla Naidoo
shamla@us.ibm.com

Shamla Naidoo, VP & Managing Partner, IBM Security. Shamla has spent her 38 year career in technology, security and privacy roles across multiple industries. In her role as Managing Partner, she advises CEOs, Board Directors and other C-suite executives on how to include security and privacy in their digital and business transformation strategies. She was formally IBM's Global Chief Information Security Officer where she was accountable to protect the IBM brands, reputation and intellectual property.

Shawn DSouza
linkedin.com/in/shawndsouza
shawn.dsouza@us.ibm.com

Shawn DSouza is the Global CTO for Hybrid Cloud Services, which is a $10B business within GBS providing cloud transformation and management services to clients worldwide. Shawn leads a global team of Distinguished Engineers and Technology leaders, with accountability for defining the technology and offering direction, and developing technical assets and accelerators to help differentiate GBS & IBM, across the Hybrid Multi-Cloud landscape. He has more than 22 years of experience in executive leadership, consulting, cloud application engineering and software product development.

Gerald Parham
linkedin.com/in/gerryparham
gparham@us.ibm.com

Gerald Parham is the Global Research Leader for Security & CIO within the IBM Institute for Business Value. Gerald's research focuses on security strategy and cyber value chains, in particular the relationship between strategy, risk, security operations, identity, privacy, and trust. He has more than 20 years of experience in executive leadership, innovation, and intellectual property development.

Research methodology

In late 2019, in collaboration with Oxford Economics, the IBM Institute for Business Value (IBV) surveyed 930 executives across 20 countries and 17 industries to better understand how cloud infrastructure, technologies, and services are influencing their security postures. Respondents included leaders of the organization's cybersecurity domain (CISOs and senior information security executives) as well as other C-suite leaders who interface directly with their organization's security leadership (CIOs, CTOs, COOs, and CEOs).

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value, part of IBM Services, develops fact-based, strategic insights for senior business executives on critical public and private sector issues.

For more information

To learn more about this study or the IBM Institute for Business Value, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and, for a full catalog of our research or to subscribe to our monthly newsletter, visit: ibm.com/ibv.

Notes and sources

1 "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations." Cybersecurity and Infrastructure Security Agency. December 17, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-352a

2 "JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA)." Cybersecurity and Infrastructure Security Agency. January 5, 2021. https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure; Bing, Christopher, Jack Stubbs, Raphael Satter, and Joseph Menn. "Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources." Reuters. February 2, 2021. https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive-idUSKBN2A22K8

3 Jensen, Benjamin, Brandon Valeriano, and Mark Montgomery. "The Strategic Implications of SolarWinds." Lawfare. December 18, 2020. https://www.lawfareblog.com/strategic-implications-solarwinds

4 Satter, Raphael, Christopher Bing, and Joseph Menn. "Hackers used SolarWinds' dominance against it in sprawling spy campaign." Reuters. December 15, 2020. https://www.reuters.com/article/us-global-cyber-solarwinds/hackers-used-solarwinds-dominance-against-it-in-sprawling-spy-campaign-idUKKBN28P2N8; Jensen, Benjamin, Brandon Valeriano, and Mark Montgomery. "The Strategic Implications of SolarWinds." Lawfare. December 18, 2020. https://www.lawfareblog.com/strategic-implications-solarwinds

5 Chappell, Bill, Greg Myre, and Laurel Wamsley. "What We Know About Russia's Alleged Hack Of The U.S. Government And Tech Companies." NPR. December 21, 2020. https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little

6 Comfort, Jim et al. "The hybrid cloud platform advantage" IBM Institute for Business Value. https://ibm.co/hybrid-cloud-platform

7 Whitmore. Wendi and Gerald Parham. "COVID-19 cyberwar: How to protect your business." IBM Institute for Business Value. https://ibm.co/covid-19-cyberwar

8 Robinson, Teri. “The cloud divide: Risks and rewards for companies that moved pre-pandemic.” *SC Magazine*. February 1, 2021. https://www.scmagazine.com/home/security-news/cloud-security/the-cloud-divide-risks-and-rewards-for-companies-that-moved-pre-pandemic

9 Comfort, Jim et al. “The hybrid cloud platform advantage” IBM Institute for Business Value. https://ibm.co/hybrid-cloud-platform

10 IBM press release. “IBM: Security in the Cloud Remains Challenged by Complexity and Shadow IT—New Data Pinpoints Top Security Risks for Companies to Address as Cloud Migration Accelerates.” June 20, 2020. https://newsroom.ibm.com/2020-06-10-IBM-Security-in-the-Cloud-Remains-Challenged-by-Complexity-and-Shadow-IT

11 Forrester. “Complexity In Cybersecurity Report 2019: How Reducing Complexity Leads To Better Security Outcomes.” May 2019. https://www.ibm.com/downloads/cas/QK1YD49A

12 Comfort, Jim et al. “The hybrid cloud platform advantage.” IBM Institute for Business Value. https://www.ibm.com/thought-leadership/institute-business-value/report/hybrid-cloud-platform

13 Nguyen-Duy. Jonathan. “Managing Today’s Risks Demands A Security Fabric Approach.” Accessed June 14, 2020. https://www.csoonline.com/article/3233293/managing-today-s-risks-demands-a-security-fabric-approach.html

14 Dotson, Chris. “Practical Cloud Security.” O’Reilly Media Inc. March 2019. https://www.oreilly.com/library/view/practical-cloud-security/9781492037507

15 Ikeda, Kazuaki, Dave Zaharchuk, and Anthony Marshall. “Three keys to competitiveness in an era of economic uncertainty.” IBM Institute for Business Value. https://ibm.co/IBV_economiccomp

16 Foster, Mark. “Building the Cognitive Enterprise: Nine Action Areas (Deep Dive).” IBM Institute for Business Value. https://www.ibm.com/thought-leadership/institute-business-value/report/build-cognitive-enterprise; Wright et al. “Accelerating the journey to HR 3.0.” IBM Institute for Business Value. https://www.ibm.com/thought-leadership/institute-business-value/report/hr-3; La Prade et al. “The enterprise guide to closing the skills gap.” IBM Institute for Business Value. https://www.ibm.com/thought-leadership/institute-business-value/report/closing-skills-gap

17 Radichel, Teri. “Exponential increases in cyber risk from Internet exposure.” Accessed June 14, 2020. https://medium.com/cloud-security/exponential-increases-in-cyber-risk-from-internet-exposure-124be0f43bf5; *Business Insider Intelligence*. “The security and privacy issues that come with the Internet of Things.” Accessed June 14, 2020. https://www.businessinsider.com/iot-security-privacy; Figure 7 - IoT vulnerabilities have increased 5400% over the last five years. “The 2019 Threat Intelligence Index.” IBM X-Force Red Vulnerability Database. Accessed September 10, 2020. https://www.ibm.com/security/data-breach/threat-intelligence

18 Crumpler, William, and James Andrew Lewis. “The Cybersecurity Workforce Gap.” The Center for Strategic & International Studies. Accessed February 22, 2021 https://www.csis.org/analysis/cybersecurity-workforce-gap

19 Sawers, Paul. “CodeSandbox launches Team Pro for whole product teams to collaborate on code in the cloud.” VentureBeat. Accessed February 22, 2021 https://venturebeat.com/2021/02/05/codesandbox-launches-team-pro-for-whole-product-teams-to-collaborate-on-code-in-the-cloud

20 Huang. Keman, Michael Siegel and Stuart Madnick. “Cybercrime-as-a-Service: Identifying Control Points to Disrupt.” Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management. Massachusetts Institute of Technology. November 2017. Accessed on June 12, 2020. http://web.mit.edu/smadnick/www/wp/2017-17.pdf; “Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar.” November 2019. Public-Private Analytic Exchange Program, sponsored by the Department of Homeland Security’s Office of Intelligence and Analysis on behalf of the Office of the Director of National Intelligence. Accessed on June 12, 2020. https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf

21 “The 2019 Cyber Resilient Organization.” Ponemon Institute and IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

About Research Insights

Research Insights are fact-based strategic insights for business executives on critical public and private sector issues. They are based on findings from analysis of our own primary research studies. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
June 2021

32038232USEN-03