Forbes insights

# Cybersecurity Trailblazers

## Make Security Intrinsic To Their Business

In association with

vmware®

## The average loss suffered from a single cybersecurity breach is now close to $4 million per incident.

There's a rising and enormous cost associated with data breaches, a trend that's driving the need for more robust cybersecurity strategies. The average loss suffered from a single cybersecurity breach is now close to $4 million per incident (up from $3.6 million last year), according to the most recent estimates from the Ponemon Institute.[1] This damage estimate includes direct costs, indirect costs and opportunity costs, including loss of customer trust.

Multiple factors are raising the risks and costs associated with cybersecurity breaches, but one thing is clear: Technology is evolving at a rapid pace, and as a result, so are cybersecurity threats.

"The technology evolution is not new, but it's accelerating," says Stuart Madnick, a professor with MIT Sloan School of Management and founding director of cybersecurity at MIT Sloan. "It opens up whole new lanes of attack surfaces that never existed before. It dramatically increases the threat landscape."

Other business environmental factors weigh in as well. "There is tremendous growth from a digital perspective, and it's compounded by a very complex regulatory landscape," says Dannie Combs, chief information security officer of Donnelley Financial Solutions (DFIN), noting that these landscapes change from year to year, if not month to month.

"It's very critical that security and business leaders understand that the security lifecycle is actually far shorter than other technology lifecycles."

[1] *2018 Cost of a Data Breach Study,* The Ponemon Institute, July 2018.

Despite these trends, the effectiveness of cybersecurity strategies and approaches still varies greatly across companies. On the one hand, many are still reactive, bolting on solutions after applications or systems have been built and deployed. Or even worse, they are treating security as an afterthought, without regard to existing technology, processes or people.

On the other hand, some enterprises are more proactive and are leading the way with more forward-looking strategies. These "cybersecurity trailblazers" are highly committed to security and consider it a core component of everything they do: entering new markets, growing and expanding products/services, increasing revenues, maintaining brand reputation and improving customer experience. In short, security is intrinsic to their business.

The best practices applied and results achieved across these different companies are explored in this report, which is based on a survey of 1,001 enterprises conducted by Forbes Insights, in partnership with VMware. The research reveals an interesting dichotomy: a clear delineation of characteristics and results between cybersecurity leaders and laggards. We also provide recommendations for how organizations can improve their enterprises' security posture and become cybersecurity trailblazers.

# Who Are Today's Cybersecurity Trailblazers?

## Cybersecurity trailblazers comprised 10% of the companies surveyed and had the following characteristics:

- **Their security organizations are involved and highly integrated** from the start in decisions across their IT technology stacks (e.g. decisions in application infrastructure and user infrastructure).
- **They consider it extremely important to have initiatives such as zero trust** and least privilege access as part of their security strategies.
- **They have high confidence** that most components of their enterprise stack—people, processes, and tools—are fully prepared to meet emerging security challenges.

# Eight Defining Features of Cybersecurity Trailblazers

**A proactive cybersecurity strategy helps prepare the enterprise to fend off ever-evolving threats,** as well as ensure that the overall attack surface remains minimized as the digital component of the enterprise expands.

Cybersecurity isn't just a technology problem: It's cultural, it's social, it's about human dynamics and it must be included as part of the business.

Here's a look at the defining characteristics of cybersecurity trailblazers and how they're meeting today's challenges with proactive measures to ensure their data and system assets are protected.

# Cybersecurity trailblazers are among the fastest-growing enterprises.

A more robust security strategy is yielding results for organizations' bottom lines, both directly and indirectly. Strikingly, cybersecurity trailblazers are 10 times more likely to be among the fastest-growing companies: 41% of trailblazers report annual growth rates exceeding 20%, compared with only 4% of their lagging counterparts.

The results seen here may reflect both direct and indirect causation patterns as enterprises with forward-looking cultures that deliver such growth are likely to be more inclined to embrace more holistic cybersecurity strategies as well. In addition, their ability to better manage risk—of which a robust cybersecurity strategy is an essential part—leads to better results in the marketplace.

41% of trailblazers report annual growth rates exceeding 20%, compared with only 4% of laggards.

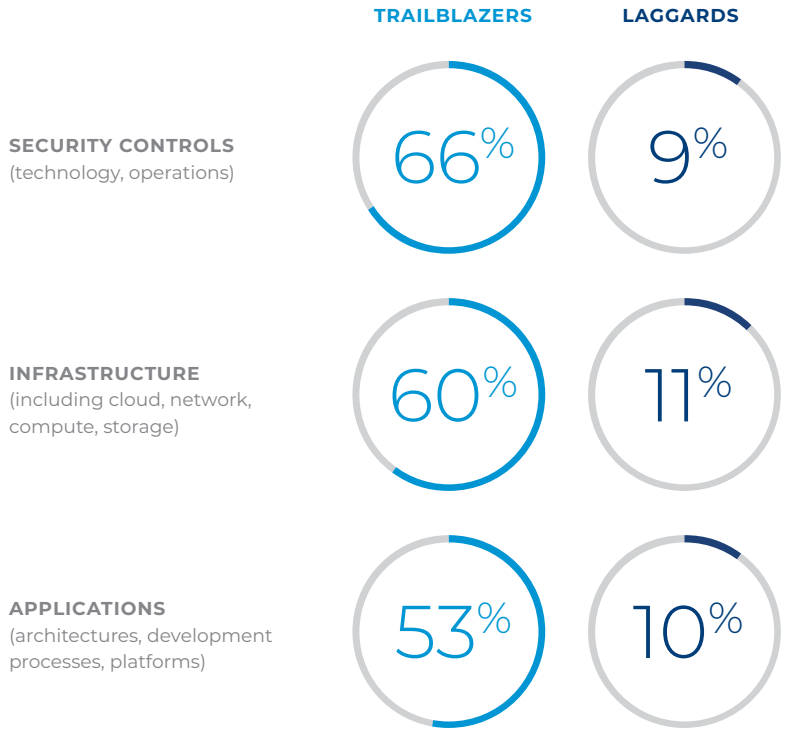
# Cybersecurity trailblazers are seeing the highest levels of transformation across their technology infrastructures that includes security controls.

Digital transformation is a force that is reshaping business technology approaches across all industries, promising greater personalization in customer engagement, more innovation in products and services, and more intelligence in operations. It's a matter of thriving and surviving in today's fast-moving economy. In a recent industry survey, 78% of executives agreed that their industry is evolving so rapidly that digital transformation is necessary for survival.[2]

Tellingly, 66% of trailblazers in the Forbes Insights survey report transformational changes in their security controls affecting both technology and operations, compared with only 9% of laggards. A majority of cybersecurity trailblazers, 60%, report transformational change taking place across their core infrastructure (including cloud, network, compute, storage), compared with 11% of lagging organizations. Applications (architectures, development processes and platforms) constitute another core area undergoing transformation, cited by 53% of trailblazers. Only 10% of less-developed organizations are seeing change in these areas. (Fig 1)

**FIGURE 1**

## Areas Seeing Transformational Change Over Last Three Years




[2] *2019 Digital Transformation Market Trends Report,* Webtorials and Masergy, February 2019.

# Cybersecurity trailblazers see security as a crucial component across their business, with a direct impact on reputation, customer experience and innovation.

Cybersecurity trailblazers are more likely to build their security strategies into their companies' business objectives as early and often as possible. Cybersecurity isn't an activity calling for additional, above-and-beyond efforts; it is an intrinsic and immutable part of their organizational fabric, from the sales floor to the C-suite.

These leaders are highly sensitive to the impact of cybersecurity on the outward projection of their companies. Almost three-fourths of trailblazers, 74%, embed security practices into efforts around maintaining brand reputation, versus 24% of laggards. In addition, 70% of trailblazers focus on the role of cybersecurity in providing superior customer experiences, versus 19% of laggards.

The all-in commitment of cybersecurity trailblazers extends just as readily to internal development and operations as well. A majority, 68%, indicate that security is an integrated part of their processes for growing and expanding their product and service lines, compared with 20% of laggards. In addition, 62% of cybersecurity leaders say security is baked into revenue-producing processes, versus 24% of laggards. (Fig 2)

**FIGURE 2**

## How Security Strategies Align With Business Objectives

For nine in 10 cybersecurity leaders, security is built into their infrastructures from the moment of inception, from data center infrastructure to mobile devices and endpoints.

Ninety-five percent of these leaders, for example, bake security into any and all network-related development and deployment, a number that's 25 percentage points higher than their laggard counterparts. Ninety-three percent of trailblazers also make security part of all device rollouts, a 20-point margin over less-developed companies.

**95%** of cybersecurity trailblazers bake security into any and all network-related development and deployment, a number that's 25 percentage points higher than their laggard counterparts.

# With an "all-in" commitment to cybersecurity, trailblazers recognize they have acute pain points that need addressing.

Perhaps because of their more sophisticated approaches to security, close to half (47%) of cybersecurity trailblazers report that they experience budget shortfalls when meeting the requirements of their security strategies, versus only 11% of laggard enterprises.

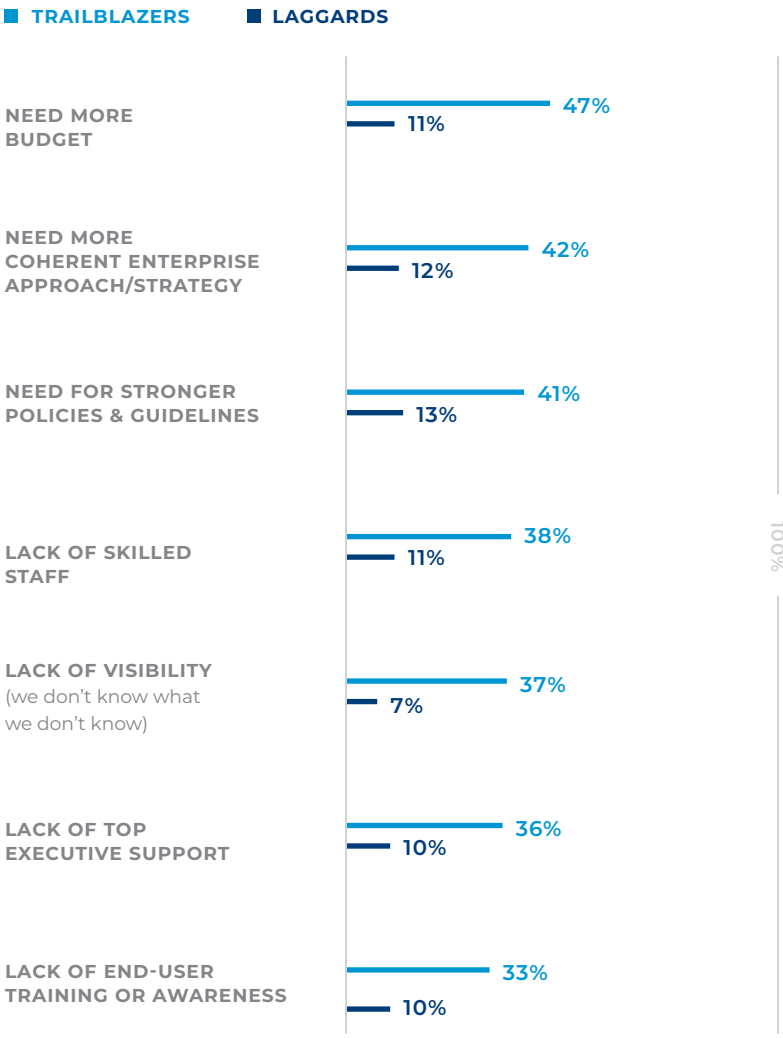
Likewise, 42% of cybersecurity trailblazers report a need for a more coherent enterprise approach and strategy, versus 12% of their less-mature counterparts—underscoring the need to align security to other technologies and business functions. (Fig 3)

Technically, managing and securing IoT or highly distributed devices presents a challenge for cybersecurity trailblazers, concerns that have yet to be fully realized by their less-developed counterparts. Forty-three percent of trailblazers report difficulty in managing devices and apps accessed from everywhere, compared with only 10% of laggards.

**FIGURE 3**

## Cybersecurity *Business* Pain Points

*Percent responding "highly represents"*



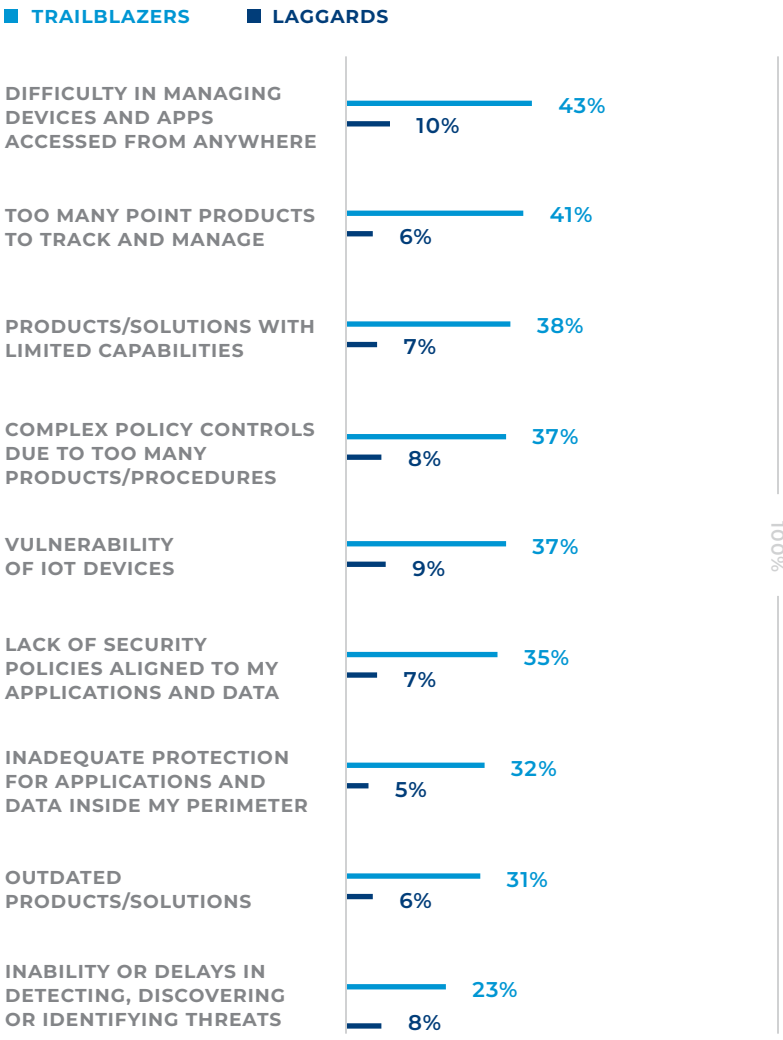
The plethora of security products now under enterprise roofs also adds to the challenge of managing cybersecurity in a cohesive way—41% of the trailblazers see this as a pain point, versus 6% of laggards. Likewise, 37% of advanced organizations say vulnerable IoT devices are a major pain point, compared with only 9% of lagging companies. (Fig 4)

Cybersecurity trailblazers also recognize that they aren't resolving issues in a timely manner. Speed of resolution is an issue, no matter how developed a cybersecurity strategy. When it comes to resolving known security issues, time is of the essence, yet 38% of trailblazers are not fully satisfied with the speed at which they can resolve issues; 28% say it takes one week or more to resolve a problem.

**FIGURE 4**

## Cybersecurity *Technical* Pain Points

*Percent responding "highly represents"*



# Cybersecurity trailblazers are highly collaborative organizations.

Companies leading in the cybersecurity realm place a premium on teamwork, not just with or among their security professionals, but across all groups within their enterprises. For architectural teams—vital for building a security culture—74% of trailblazers cite their security roles as "highly collaborative," versus 13% of laggards.

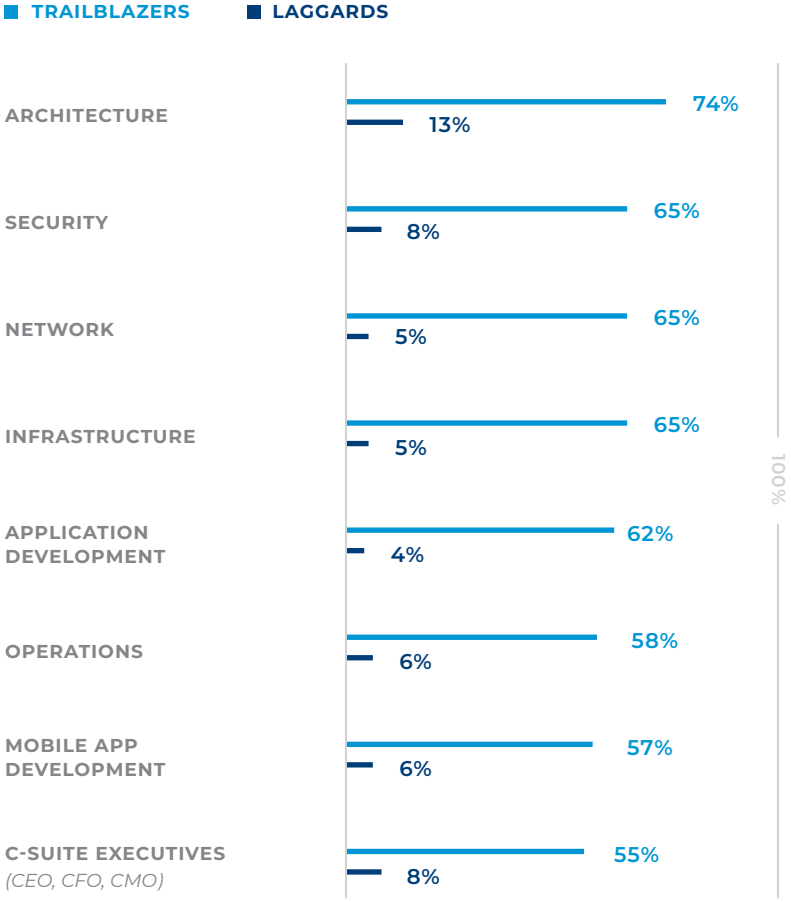
For other types of professional teams, the differences are similarly stark. Nearly two-thirds of trailblazers, 65%, rate their security teams as "highly collaborative," versus only 8% of laggards. The same applies to their infrastructure teams—65% say these teams are highly collaborative on security matters, versus 5% of lagging companies.

C–suite executives also join in on security collaboration within cybersecurity trailblazing organizations, as cited by 55%. By contrast, only 8% of lagging organizations see such levels of collaboration among their senior executives. (Fig 5)

**FIGURE 5**

## Organizational Collaboration in Addressing Security Concerns

*Percent reporting high levels of collaboration*



Collaboration on cybersecurity requires training and knowledge at all levels, and leading organizations make this a firm part of their working relationships. "The entire organization must be committed to security to be successful," says Combs. "If you look at the risk landscape today, the entire enterprise gamut has been targeted."

At DFIN, information security awareness is something that is expected of everyone, he continues. "Anyone who has access to our environment—employee, contractor or even a vendor—will go through the DFIN security awareness training program. That's a firm expectation we put in place."

> "The entire organization *must be committed* to security to be successful."

Dannie Combs
Chief Information Security Officer, DFIN

## While cybersecurity trailblazers focus most of their security controls on infrastructure, they seek a more balanced approach that extends to users and applications.

Cybersecurity trailblazers are committed to a proactive strategy that seeks to reduce the scope of their attack surface, as well as threat hunting.

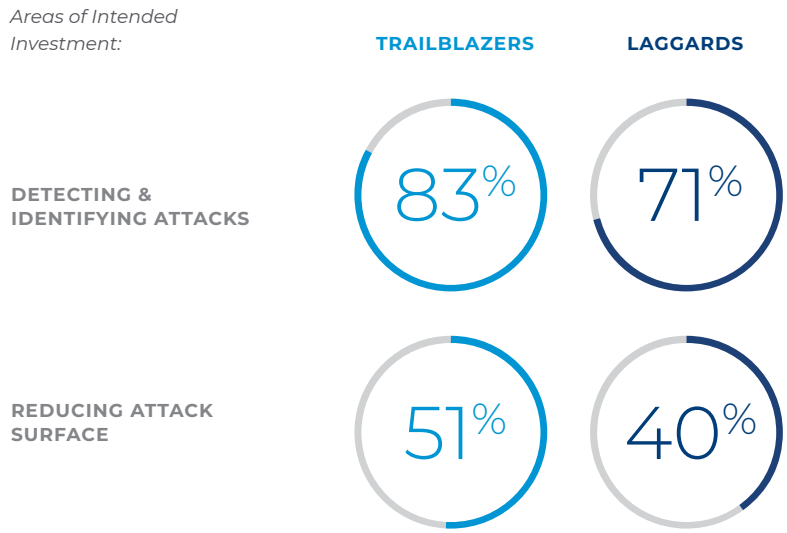
A majority of these leaders, 51%, intend to invest more in a holistic strategy that decreases their attack surface (versus 40% of lagging companies). (Fig 6)

Executives were also asked about the concentration of their security controls. Close to half of the trailblazers, 46%, report their security controls are aligned to their infrastructure, while 35% focus them on user access; only 18% align to applications and data.

There is recognition, however, that this must change, and in three years, 41% of trailblazers seek to better align security controls to applications and data.

**FIGURE 6**

### Cybersecurity Trailblazers Seek More Proactive Security Investments



# Cybersecurity trailblazers are investing heavily in proactive measures.

One-third of trailblazers, 33%, report plans to increase spending on upgrading security solutions by more than 20% over the next three years, compared to 8% of lagging organizations.

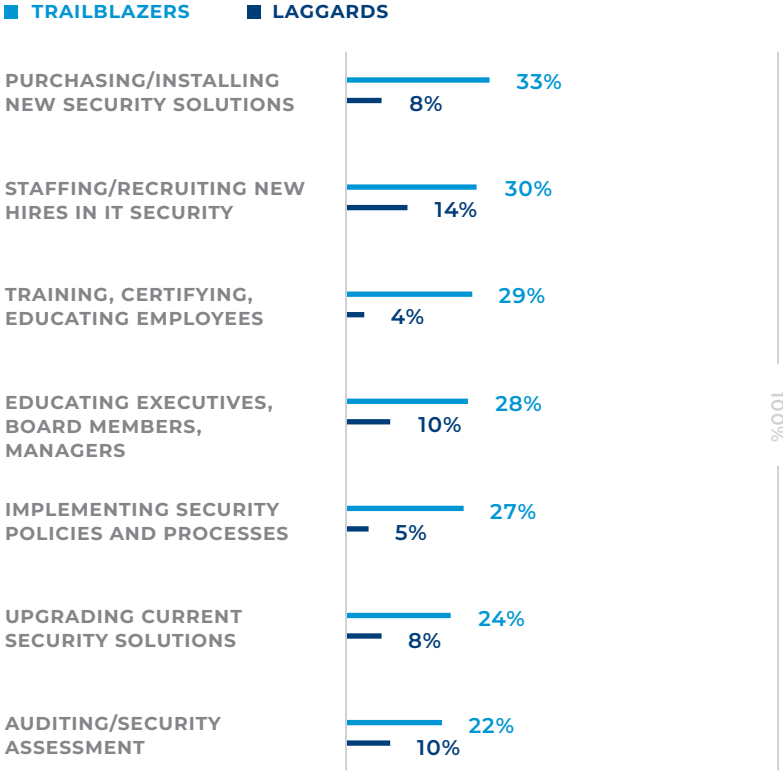
A similar percentage of trailblazers intend to significantly increase their investments in people. Thirty percent are increasing funds for cybersecurity staffing, more than double their lagging counterparts.

In addition, 29% of trailblazers will be ramping up their investments in training, versus only 4% of laggards. Another 28% will be devoting a large commitment of resources to executive education, compared to 10% of their less-cybersecurity savvy counterparts. (Fig. 7)

**FIGURE 7**

## Where High Levels Of Investment in Cybersecurity Will Take Place Over The Next Three Years

*Percent expecting increases greater than 20%*

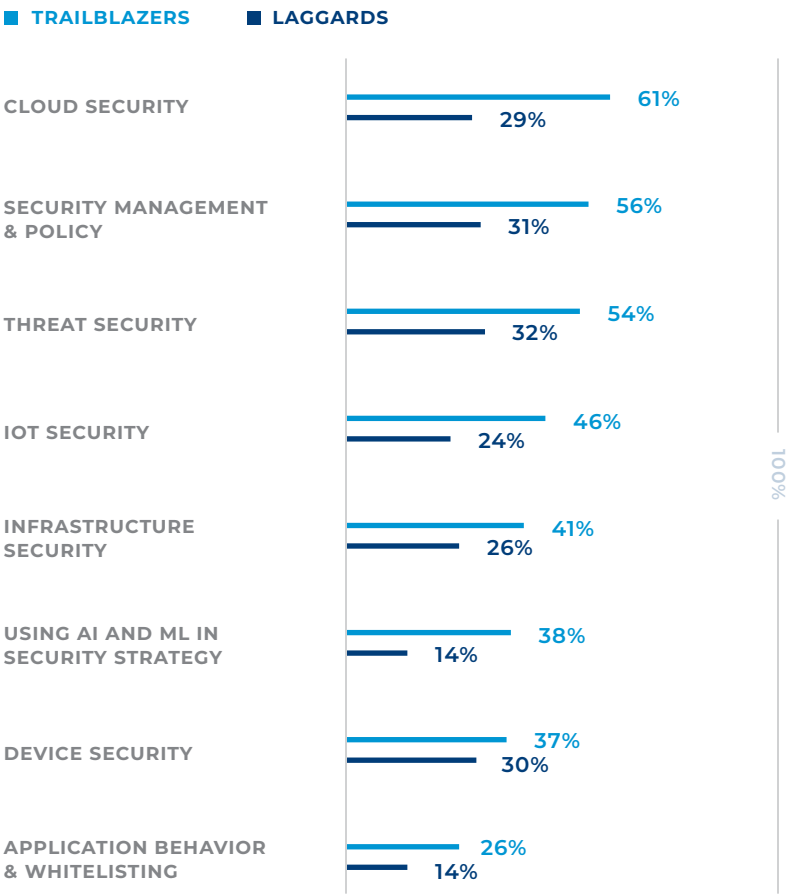


Cloud security tops spending plans over the next three years. Sixty-one percent of leaders plan to invest more heavily in cloud security, compared to 29% of laggards.

More than half, 56%, will also be investing more in security management and policy. By contrast, 31% of less-advanced companies plan to invest in this area. (Fig. 8)

**FIGURE 8**

## Top Security Projects That Will Be Invested In Over The Next Three Years



# Cybersecurity trailblazers recognize the power and advantages of the cloud, but are cautious about turning over too much security to cloud providers.

While 94% of leaders are employing cloud services for some aspects of security, they understand that handing over the keys to their enterprise is abdicating responsibility. Executives within leading companies have concerns about cloud, citing the potential inability to control the elements of the infrastructure end to end, cited by 49% versus 37% of laggards.

As a result, leading companies are less prone to outsource their security to cloud providers. Only 31% of leaders report turning over "many" security measures to cloud providers.

Load balancing and endpoint detection and response are the leading core security functions trailblazers have put into the cloud. Tellingly, these leaders are on a par with, or less inclined than, their laggard counterparts to be adopting cloud for core security functions: 36% of trailblazers use cloud exclusively for load balancing, versus 28% of laggards. Endpoint detection and response is cloud-based for 34% of trailblazers, versus 30% of laggards. At the same time, laggards have been more likely to adopt cloud services to handle their secure web gateway (34% of laggards versus 27%) and identity management (30% versus 21%).

# How To Become A Cybersecurity Trailblazer

**Clearly, a distinguishing characteristic of a cybersecurity trailblazer** is an understanding that security must be intrinsic across all levels of the business—from technology to processes to people and culture. It's also clear that those that adopt this mindset are more aligned to business objectives, and security plays an important role in business growth.

The following are suggestions for improving enterprises' security posture, based on lessons learned from the cybersecurity trailblazers and executives interviewed for this report.

# HOW TO BECOME A CYBERSECURITY TRAILBLAZER

**Start now to make cybersecurity an integral part of corporate culture.** The jobs of security proponents are that much harder if they are working against an unresponsive organization that treats cybersecurity measures as one-off projects.

"If you can't find a way as an organization or as a chief security officer to connect security into your core strategy—so everyone knows this is part of 'who we are' and 'what we do'—you will have a much steeper hill to climb and a lot more risk," says Steve Martino, chief information security officer for Cisco. "You can't be the choke point if business is going to move fast. You have to make security part of the fabric of the company. You have to embed security into the processes of the company."

It's also important to recognize that building a cybersecurity-aware culture is a long-term process. As Madnick points out, this represents "a dramatic change in thinking in many companies and not an easy change to make. Think about manufacturing, which has a safety culture that has evolved over time. You often see a sign over factory doors that says, 'It's been 500 days since our last industrial accident.' When was the last time you went into a data center and saw a sign that said, 'It's been 15 milliseconds since our last cyberattack'? It took two, three, four decades to develop a safety culture and awareness in manufacturing. We can speed the process up, but it's going to be a nontrivial process to develop a cyber-aware, cyber-safe culture in organizations."

> If you can't find a way as an organization or as a chief security officer to *connect security into your core strategy*—so everyone knows this is part of 'who we are' and 'what we do'—you will have a much steeper hill to climb and a lot more risk."

Steve Martino,
Chief Information Security Officer, Cisco

# HOW TO BECOME A CYBERSECURITY TRAILBLAZER

**Encourage and reward greater collaboration with and beyond security teams.** As data, systems and applications touch every corner of the business, security needs to be an enterprise effort led by C-suite executives and even members of the board of directors.

Yet at this time, only one in four executives and practitioners are seeing high levels of collaboration, the Forbes Insights survey shows. There is impetus for greater cross-enterprise collaboration building: More than 70% of executives are looking at adopting a model around DevSecOps—in which development, operations and security teams collaborate in application rollouts—to provide better integration and business value.

The growing complexity of today's systems and applications demands such collaboration. "Get connected with your developers and build security into their daily processes," urges Nathan Wenzler, senior director of cybersecurity at Moss Adams. "More and more applications are being attacked because they're not being coded with security in mind. Going forward, the complexity of these applications will make it easier for attackers to find ways to compromise them and gain access to data or systems. Security teams need to work hand-in-hand with developers to make sure their applications are as resilient as possible."

Weaving security throughout the software development lifecycle is key to this cross-enterprise collaboration, Combs adds. "Bake in security through your ideation, development, deployment as well as support processes."

>70%

of executives are looking at adopting a model around DevSecOps—in which development, operations and security teams collaborate in application rollouts—to provide better integration and business value.

# HOW TO BECOME A CYBERSECURITY TRAILBLAZER

**Develop a proactive security strategy that focuses on reducing an enterprise's attack surface, versus attempting to chase individual threats.** The key is to narrow hackers' or bots' options to take down the network. Still, many companies are challenged due to the expanding adoption of technology, such as cloud, mobile and IoT—unwittingly expanding their attack surface. Changing this paradigm requires committing resources and investments in a holistic, forward-looking approach to security, versus constant firefighting.

Tellingly, the question of how much to invest in cybersecurity is an open one, Madnick points out. "Whether they're investing enough, I'm almost sure the answer is no," he says. "Are they investing in the wrong places? The answer is probably yes. Part of the reason is they're reacting, rather being proactive. They're doing things after the fact, rather than before the fact. What tends to happen is most organizations invest predominately in protective features or prevention methods—they're putting in stronger locks but still leaving their keys under the mat.

Executives need to understand what things need the most protection, the crown jewels. It's the exceptional organization that's really thought that through."

---

**Invest in cybersecurity talent and knowledge at all levels.** Moving forward with a comprehensive cybersecurity strategy requires engagement at all levels of the enterprise.

This occurs at two levels—building the technical proficiency of IT staff members, as well as promoting awareness and vigilance among the business workforce. The greatest threats come from a lack of employee or end-user awareness or training to deal with ongoing cybersecurity threats.

An investment in training and awareness may be a cost-effective way to prevent unwanted code corrupting corporate systems. Just as police rely on citizen engagement and watchfulness to prevent and fight crime in their communities, enterprises need the full engagement of their employees. "There's a tendency to believe that it's a technical issue, so IT can solve all the problems," says Madnick. "Everybody plays a role."

# HOW TO BECOME A CYBERSECURITY TRAILBLAZER

**Look to the cloud for enhanced security options.** Because it is so critical to their business, cloud providers are constantly updating their technologies, skills and certifications to ensure that their clients' data and applications have the latest and best possible security profiles. According to the Forbes Insights survey, a third of cybersecurity trailblazers put endpoint detection and response in the cloud. In addition, cloud providers may provide enhanced endpoint detection, threat intelligence, analytics services and many others. Cloud provides an option for enterprises seeking optimum cybersecurity capabilities, and options can be adjusted based on factors such as budget, in-house expertise and staffing.

---

**Collaborate with cloud providers on security, but maintain due diligence.** Many enterprises find it more effective to turn over the nuts and bolts of security work to cloud providers. However, ultimate responsibility for security should not be outsourced. Rather than rely on providers' security promises, enterprise managers need to work closely and collaboratively with cloud providers to understand what level of security they are providing to identify any potential gaps.

Cloud security is a top concern and area of focus for trailblazers. Sixty-one percent of these leaders say it's extremely important for security to be an intrinsic part of their cloud infrastructure—and the same percentage of them report having highly collaborative teams around application development (62%). It's important to factor security into all aspects of application management, whether in the cloud or on-premises. If you are using the cloud and cloud services, it's important that your security approach and strategy extend to this area. Compliance, maintaining configurations and avoiding shadow IT are all part of the due diligence.

The depth and degree of reliance on cloud security varies from situation to situation. "It depends on the cloud provider that you select, the business challenges you're trying to solve and the security talent you have on staff," says Combs. "With cloud, you can subscribe to security services and hold a vendor accountable to security SLAs, and therefore have less worry regarding the operational oversight of a security control." However, "with the cloud also comes new technologies, which bring unknown vulnerabilities," Combs adds. "It's important that your team understands those technologies well and architects around those vulnerabilities. One of the biggest challenges to cloud relative to security is there's just not enough expertise for the cloud—particularly with identity and access management."

# HOW TO BECOME A CYBERSECURITY TRAILBLAZER

**Adopt automation and intelligent analysis to manage security.** Automated incident response and patching provides enterprises with the ability to respond, in real time, to the plethora of threats and incidents surging through today's networks. Artificial intelligence and machine learning—seen through AIOps—enables the standardization and automation of IT service delivery. These automated tools provide enterprises with visibility into cybersecurity threats.

Combs' team is building its security architecture around SOAR, oor security orchestration, automation, and response, which focuses on automating much of the cybersecurity threat mitigation process. "This is about understanding fundamental risks, building an automated script playbook that executes under certain conditions and systematically mitigates well-known risks," says Combs.

**Continually reevaluate, improve, and simplify security architecture.** The only constant in cybersecurity is change. Not only are threats constantly evolving, but businesses are rapidly changing as well. "Business landscapes change every year," Combs says. "There's such tremendous growth from a digital perspective, compounded by a very complex regulatory landscape. The tools, techniques and technologies used by bad actors are changing just as quickly." To help the organization move forward, there needs to be greater integration—or consolidation—of security tools. Security tools need to be orchestrated to reduce complexity. If you make security intrinsic to the business, it stands to reason that the approach will change and adapt as your business priorities shift.

# METHODOLOGY

Forbes Insights surveyed 1,001 executives from across the globe representing manufacturing, retail, financial services, healthcare, government and education. More than four in 10 respondents were from the C-suite (including chief information security officers, chief information officers and chief technology officers), and nearly a quarter were in security management roles. Responses were weighted to reflect market size.

# ACKNOWLEDGMENTS

Forbes Insights and VMware would like to thank the following individuals for their time and expertise:

**Dannie Combs**
Chief Information Security Officer, Donnelley Financial Solutions

**Stuart Madnick**
Professor with MIT Sloan School of Management; Founding Director of Cybersecurity at MIT Sloan

**Steve Martino**
Chief Information Security Officer, Cisco

**Nathan Wenzler**
Senior Director of Cybersecurity, Moss Adams

**Forbes insights** is the strategic research and thought leadership practice of Forbes Media, a global media, branding and technology company whose combined platforms reach nearly 94 million business decision makers worldwide on a monthly basis.

By leveraging proprietary databases of senior-level executives in the Forbes community, Forbes Insights conducts research on a wide range of topics to position brands as thought leaders and drive stakeholder engagement. Research findings are delivered through a variety of digital, print and live executions, and amplified across Forbes' social and media platforms.

---

Report Author:
**Joe McKendrick**

499 Washington Blvd. | Jersey City, NJ 07310 | 212.367.2662 | https://www.forbes.com/forbes-insights/