FORRESTER®

The Rise Of The Business-Aligned Security Executive

The Bad News? There's A Disconnect Between Business And Cybersecurity. The Good News? Aligning Them Can Make All The Difference.

Get started →

FORRESTER THOUGHT LEADERSHIP PAPER: A CUSTOM STUDY COMMISSIONED BY TENABLE | AUGUST 2020

Today's CISOs And Other Security Leaders Must Translate Cybersecurity Threats Into The Language Of Business Risk

We live in the era of the digital business, which operates on a complex, dynamic, and highly fragmented matrix of on-premises, cloud, and hybrid infrastructure, applications, data, mobile, internet of things (IoT), and IT/OT converged systems. Every digital business must protect this sprawl of interconnected technologies that make up the modern attack surface. Yet for all the industry's cybersecurity advances and investments, there is a massive disconnect in how businesses understand and manage cyber risk.

Digital transformation has woven the threads of intellectual property and technology together. The modern CISO can no longer focus on just one thread; s/he must advocate for security of both the technology and the business — evolving from a technology expert to a business-aligned security leader.

COVID-19 Offers A Concrete Example Of The Disconnect Between Business And Security

Forty-one percent of decision makers report that their firms had experienced at least one business-impacting cyberattack related to COVID-19 in the prior 12-month period, as of April 2020.

Although 96% of respondents have developed COVID-19 response strategies, business and security are not closely aligned: 75% of business and security leaders say their COVID-19 response strategies are only "somewhat" aligned, at best.

Key Findings

Tenable commissioned Forrester Consulting to conduct an online survey of 416 security and 425 business executives, as well as telephonic interviews with five business and security executives, to examine cybersecurity strategies and practices at midsize to large enterprises. The study, conducted in April 2020, revealed four key takeaways:

1

Cybersecurity threats thrive amid a climate of uncertainty, making it a topic worthy of board-level visibility. **Most executives (94%)** say their firms have experienced a business-impacting cyberattack or compromise within the past 12 months — that is, one resulting in a loss of customer, employee, or other confidential data; interruption of day-to-day operations; ransomware payout; financial loss or theft; and/or theft of intellectual property. Roughly **two-thirds (65%)** say these attacks involved operational technology (OT) assets.

2

Business leaders want a clear picture of their organizations' cybersecurity posture, but their security counterparts struggle to provide one. Just **four out of 10 of security leaders** say they can answer the question, "How secure, or at risk, are we?" with a high level of confidence.

3

There is a disconnect in how businesses understand and manage cyber risk. **Fewer than 50% of security leaders** are framing the impact of cybersecurity threats within the context of a specific business risk. **Only half (51%)** say their security organizations work with business stakeholders to align cost, performance, and risk reduction objectives with business needs. **Four out of 10 (43%)** report they regularly review the security organization's performance metrics with business stakeholders.

4

Cybersecurity needs to evolve as a business strategy. This can't happen until security leaders have better visibility into their attack surfaces. **Just over half of security leaders** report that their security organizations have a holistic understanding and assessment of their firms' entire attack surfaces, and **fewer than 50% state that their security organizations** are using contextual threat metrics to measure their firms' cyber risk. This means their ability to analyze cyber risks and prioritize and execute remediation based on asset criticality and threat context is limited.

> **We don't have hard and fast data for making assumptions about [risk]. That is always problematic, especially if we're escalating risks to an executive management team. If you don't feel confident in the source of that data, then you're not going to inspire confidence that the things you're doing to reduce risk are appropriate.**
>
> — VP and chief information security officer, business process outsourcing and human capital management

The Future Belongs To The Business-Aligned Security Leader

When security and business leaders are aligned on agreed-upon contextual data, they deliver significant, demonstrable results:

Business-aligned security leaders are **eight times** as likely as their more siloed peers to be highly confident in their ability to report on their organizations' level of security or risk.

Most execs at business-aligned organizations (80%) report having a business information security officer (BISO) or similar title, compared with only 35% of their less-aligned counterparts.

Business-aligned security leaders are also more likely than their more reactive counterparts to have a defined benchmarking process: **86% have a process that clearly articulates expectations** and demonstrates continuous process improvement relative to peer companies and/or internal groups, compared with just 32% of their non-aligned peers.

Business-aligned security leaders outpace their more reactive and siloed counterparts in automating key vulnerability assessment processes by margins of **+49 to +66 percentage points.**

85% of business-aligned security leaders have metrics to track cybersecurity ROI and impact on business performance versus just 25% of their more reactive and siloed peers.

To achieve alignment, CISOs and other security leaders need the right combination of technology, data, processes, and people.

Cybersecurity Threats Thrive Amid A Climate Of Uncertainty

We struggle to predict the future, now more than ever. Even the nature of work is shifting rapidly and without warning. But in this time of uncertainty, there is one thing enterprises can count on: Cyberthreats will proliferate, exposing every organization to significant business risk. Nearly every security and business leader says their organization had experienced a business-impacting cyberattack or compromise within the past 12 months, i.e., one resulting in a loss of customer, employee, or other confidential data; interruption of day-to-day operations; ransomware payout; financial loss or theft; and/or theft of intellectual property. Nearly half weathered five or more attacks. Further, more than two-thirds of executives say business-impacting cyberattacks have increased over the past two years — a grim trend roughly eight out of 10 executives expect will continue over the next 24 months.

> **"We are more at risk. . . . Those risks, outside of our four walls, are continuously elevating."**
> — Chief financial officer and chief operating officer, retail

94%
experienced a business-impacting cyberattack or compromise within the past 12 months; **46%** weathered five or more attacks.

65%
say attacks involved OT assets.

68%
of organizations have seen an increase in business-impacting cyberattacks over the past two years.

77%
expect an increase in cyberattacks over the next two years.

Base: 841 security leaders and business executives with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

Enterprises Battle Many Forms Of Business-Impacting Attacks

Enterprises are not only combating a greater number of cyberattacks, but the types of attacks are more varied, with the average organization experiencing five different methods of attack. According to the executives we surveyed, fraud, data breaches, ransomware, and software vulnerabilities were among the most common types of attacks executed on enterprises over the past 12 months. Despite being just months into 2020, a surprising 41% of execs say their organizations fell victim to pandemic-related malware or phishing — making it the No. 1 mode of compromise.

63%

of security leaders admit it's likely their systems suffered an unknown compromise over the past year.

Top 5 business-impacting cyberattacks or compromises

1. **41%** Malware or phishing (related to COVID-19)
2. **40%** Fraud
3. **37%** Data breach
4. **36%** Ransomware
5. **34%** Software vulnerability

"The No. 1 way into our organization is a phishing email or call . . . and I think they're increasing with coronavirus."

— Director, information security, manufacturing

Base: 795 security leaders and business executives with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

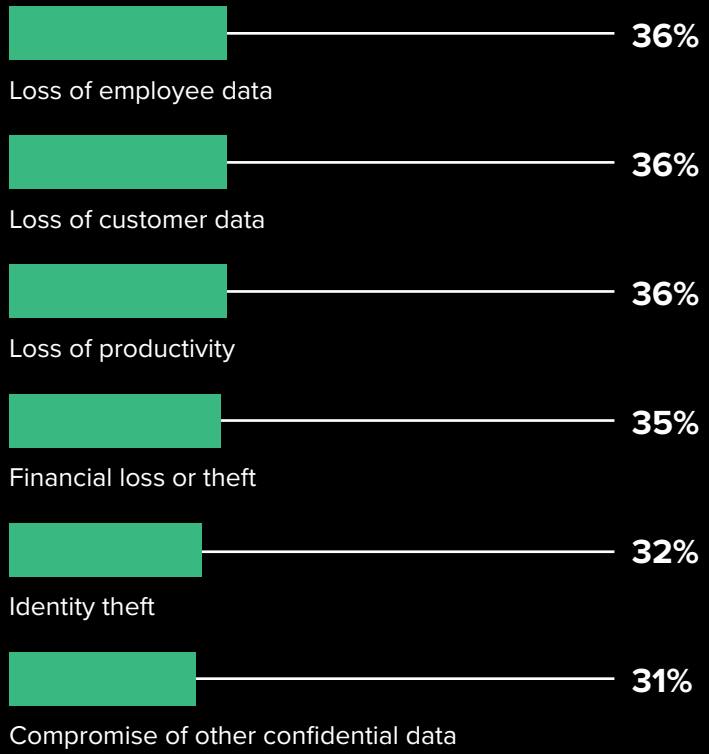
Loss Or Compromise Of Data Tops The List Of Business-Impacting Events

Organizations rarely emerge unscathed from a cyberattack, and respondents' organizations are no exception: Just 1% of business and security leaders say the attacks and compromises of the past year have had no impact.

Cyberattacks can have a damaging impact on the business. While loss of productivity, financial loss, and identity theft are among the top consequences of attacks, over one-third of surveyed executives reported a loss of employee or customer data, and 31% experienced compromise of other confidential data.

> **"The store burns down; it's a store, and I move on. Someone gets into my house file with all my customers, and that's an entirely different exponential exposure."**
>
> — Chief financial officer and chief operating officer, retail

"How did these attacks or compromises impact your organization?"



Note: Multiple responses allowed; responses over 30% shown
Base: 795 security leaders and business executives with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

Business Leaders Want A Clear Picture Of Their Firms' Cybersecurity Posture

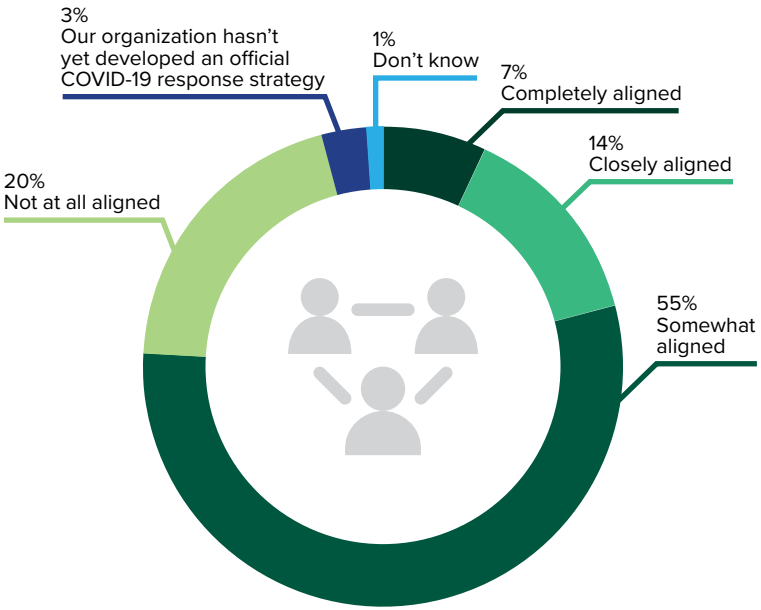
Security leaders are called upon to keep business leaders and board members apprised of their organizations' threat posture, but many struggle to obtain an answer to that question, let alone accurately communicate this information.

Our study revealed that **just four out of 10 of security leaders can answer the question, "How secure, or at risk, are we?" with a high level of confidence**. Further, a whopping 66% of business leaders are — at most — only somewhat confident in their security teams' ability to quantify their organizations' level of risk or security. In the current climate of uncertainty triggered by the global COVID-19 pandemic, digital business clearly requires a new way to measure and manage cybersecurity as a strategic business risk.

75%

of business and security leaders say their COVID-19 response strategies are, at best, only "somewhat" aligned.

"How closely aligned are your cybersecurity and business leaders in developing a COVID-19 response strategy?"



Base: 593 security leaders and business executives with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

There Is A Disconnect In How Businesses Understand And Manage Cyber Risk

Reactive, siloed, and tactical security strategies hinder security leaders' ability to get a clear picture of their organizations' cybersecurity health and an understanding of which threats pose the greatest business risk.

The study revealed a core issue: Cybersecurity initiatives are seldom aligned with business objectives. Security leaders are challenged to prioritize where they focus — not just when it comes to vulnerabilities but their entire cybersecurity strategy in general. When this strategy is disconnected from business goals, the message of risk is often lost in translation.

RESPONSE TO THE COVID-19 PANDEMIC OFFERS A CONCRETE EXAMPLE OF THIS DISCONNECT

The COVID-19 pandemic presented malicious actors an opportunity to infiltrate organizations as enterprises scrambled to adapt to "business-as-*un*usual." As previously discussed, four out of 10 business and security leaders report having experienced COVID-19-related malware or phishing attacks; an unlucky 10% were victims of both. Surprisingly, even though 96% of execs say their organizations have developed an official COVID-19 response strategy, business and cybersecurity strategies fail to connect: 75% of business and security leaders say their COVID-19 response strategies are, at best, only "somewhat" aligned.

> **“There are two languages getting spoken. Business leaders want to know, ‘What’s the cause, what’s the headline, what’s the risk?’ The language barrier between [business and security leaders] is a chasm.”**

— Business information security officer, financial services

Business And Cybersecurity Strategies Are Seldom On The Same Page

Six out of 10 business executives report their security leaders are, at best, only somewhat effective in communicating the risk cybersecurity threats pose to their organizations. So, what's the disconnect? The study revealed:

- Just 54% of security leaders and 42% of business executives say their cybersecurity strategies are completely or closely aligned with business goals.
- Fewer than half of security leaders consult business executives all the time or very frequently when developing their cybersecurity strategies.
- On the flip side, four out of 10 business executives rarely — if ever — consult with security leaders when developing their organizations' business strategies.
- Just 47% of security leaders say they always or very frequently consider business priorities when defining cybersecurity priorities.
- Fewer than half of security leaders are framing the impact of cybersecurity threats within the context of a specific business risk.

Security Leaders Need To Speak The Language Of Business Risk

"For the business leaders, money's the currency — literally and figuratively. That will [make risk] resonate for them. The technical needs to go out the window entirely. No one understands it; no one cares. They care about dollars to their bottom line."

— Chief financial officer and chief operating officer, retail

"[Business leaders] have the capability but not the know-how. . . They don't understand the value [of cybersecurity] unless it's in their language. They don't own the risk because they don't understand it belongs to them."

— Business information security officer, financial services

"You need to message it to [business executives] so they receive it. At the same time, don't sell them fear — fear shuts people off. They say, 'You're full of it, you're paranoid, you're crying wolf. No way.' If you start saying, 'We probed your system and we found these holes,' that becomes real."

— Chief operating officer and VP system operations, healthcare

"If you're going to sit in the C-suite and talk about what you're doing, if you've lined it up with what the organization has committed to being its key objectives, then that conversation will be easier."

— Vice president and chief information security officer, business process outsourcing and human capital management

"If you address the high-priority business risks and align your security program with those, you're going to get a lot more buy-in from the executive team."

— Director of information security, manufacturing

Security Leaders Have An Incomplete Picture Of Their Attack Surfaces And Criticality Of Assets

To be effective strategic partners to the business, security leaders must have a holistic understanding of all their entire attack surfaces within the context of business risk. And while these leaders have been given the remit to manage risk across the entirety of their organizations' critical assets, ecosystem complexity and limited visibility hinder their efforts.

CONVEYING THE LEVEL OF BUSINESS RISK IS DIFFICULT DUE TO THE COMPLEXITY OF THE MODERN ATTACK SURFACE ENTERPRISES MUST PROTECT

Security organizations must protect a dynamic and highly fragmented matrix of on-premises, cloud, and hybrid infrastructure, applications, data, mobile, IoT, IT, and OT systems — not to mention employees, contractors, and third-party partners.

Not only did the pandemic force organizations to rethink how they do business, but it also made it even more challenging for security teams: 64% of execs say their organizations currently include remote and/or work-from-home employees in their attack surfaces. In fact, 67% of leaders are very or extremely concerned that COVID-19-related workforce changes will further increase their organizations' level of risk.

> **"There are security gaps whenever anyone works at home, but now it's just a very large scale [with COVID-19]. . . . You have to learn how to take care of your attack surface."**
>
> — Business information security officer, financial services

AN INCOMPLETE VIEW INTO ENTERPRISE ASSETS PREVENTS A HOLISTIC UNDERSTANDING OF RISK

Limited visibility into assets beyond the traditional perimeter make it difficult for security teams to comprehensively assess risk: Employees, partners, and contractors — as well as mobile and IoT technologies — expose enterprises to considerable risk. The study found:

- While roughly 70% or more of security leaders say they have high or complete visibility into their organizations' applications, data, IT, and cloud platforms, just six out of 10 have a similar level of visibility into OT, IoT, and mobile devices.
- Six out of 10 report high or complete visibility into on-premises employees to assess risk, but only 52% can say the same when employees are remote or working from home.
- Security organizations have limited visibility to assess the risk posed by contractors and third-party partners and vendors, with just 51% and 55%, respectively, reporting high or complete visibility into these parties.

As a result, few security leaders have a holistic understanding of their organizations' attack surfaces and most critical assets.

Just

53%

report that their security organization has a holistic understanding and assessment of the organization's entire attack surface.

Only

44%

say their security organization has good visibility into the state of security for their organization's most critical assets.

Note: A rating of 4 or 5, where 5 is "completely describes my organization"
Base: 416 security leaders with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

"We have blind spots. . . . We're trying to get to a point where all assets are regularly assessed from a risk perspective, but that's a challenge especially with technology where it's not something that's necessarily constantly connected and has a static IP address and location. So mobile devices and the kind of equipment that changes locations are really difficult to keep track of."

— VP and chief information security officer, business process outsourcing and human capital management

"We're getting software for our X-ray machines, our CTs, our pump upgrades. [Hackers have] tacked on to those files, and something that you would anticipate was securable is not."

— Chief operating officer and VP of system operations, healthcare

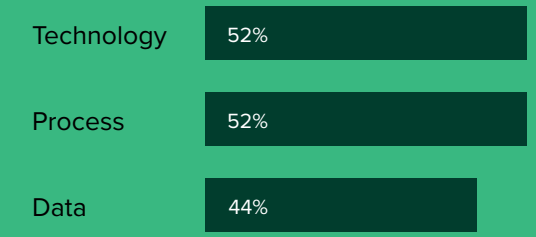
Security Leaders Lack Confidence That Current Tools Can Predict Business-Impacting Cybersecurity Threats

Security leaders must ensure their organizations are prepared to tackle oncoming threats, but many lack the technology, data, and processes to do so. Over half of security leaders lack confidence they have the technology or processes to predict cybersecurity threats, and roughly two-fifths are unsure they have the necessary data.

This could, in part, be due to a lack of vulnerability management (VM) process automation: No more than half of security leaders say they have significantly automated VM assessment processes. Of note, only 44% of security leaders apply business risk management objectives to vulnerability prioritization practices. Additionally, three out of 10 security decision makers say their firms still primarily use manual reviews of spreadsheets to track cybersecurity performance.

"How confident are you that your security organization has the technologies, processes, and data to accurately predict the likelihood of a cybersecurity threat impacting the business?"

(Showing somewhat, not that, or not at all confident responses)



36%

describe their cybersecurity strategy as largely reactive and focused on solving the problem of the day, rather than predictive or forward-looking.*

*Note: A rating of 4 or 5, where 5 is "completely describes my organization"
Base: 416 security leaders with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

Cybersecurity Metrics Often Lack Business-Risk Context

Few security organizations use threat metrics that speak to business risk. At the heart of the issue is a lack of partnership between security and business leaders to ensure alignment between cybersecurity metrics and objectives with business priorities. The study revealed:

- Only half of security leaders say their security organizations work with business stakeholders to align cost, performance, and risk reduction objectives with business need.
- Four out of 10 report they regularly review the security organization's performance metrics with their business counterparts.

The security organization works with business stakeholders to align cost, performance, and risk reduction objectives with business need.*

The security organization regularly reviews its performance metrics with business stakeholders.*

Fewer than

50%

of security organizations are using threat metrics that incorporate business risk context to measure their organizations' cyber risk.

*Note: A rating of 4 or 5, where 5 is "completely describes my organization"
Base: 416 security leaders with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

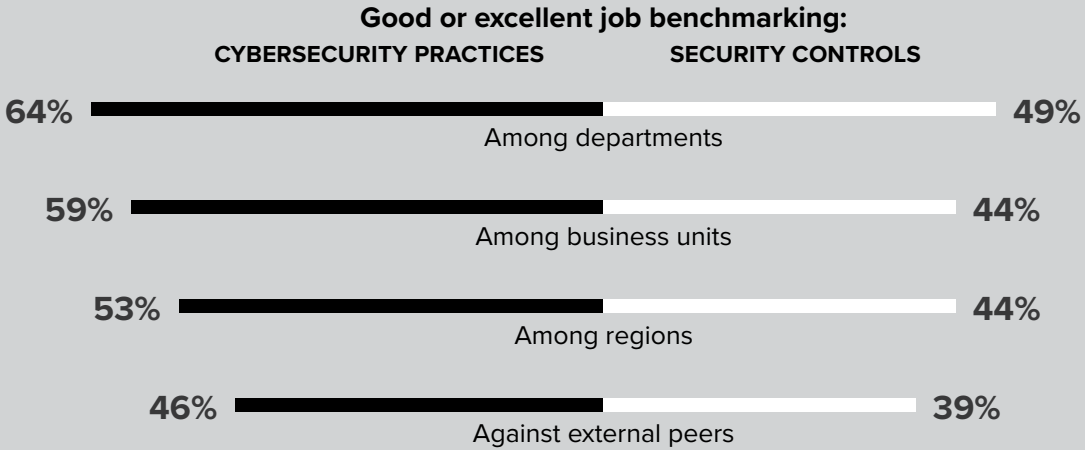
> **“As a leader, you have to have some kind of report card with lots of components going into the grades. Are you enabling the business, as you move forward with agility? Are you keeping your business safe? Cyber risk should be weighted appropriately against that.”**

— Business information security officer, financial services

A Limited Approach To Benchmarking Makes It Difficult To Communicate Business Risk

Many security leaders fall short when benchmarking their cybersecurity programs against external data — or even against internal peers. Benchmarking against industry frameworks can be useful but may be highly qualitative and limited by the scope of the database used; fewer than half of security leaders consider the industry benchmarking frameworks they use to be very effective in accurately reporting on business risk.

Security organizations lack consistent proficiency in benchmarking security practices. While over half of security leaders give themselves good marks for internal benchmarking practices, just 46% rate their capability to benchmark cybersecurity practices against external peers as good or excellent. Similarly, fewer than half say they are doing an adequate job benchmarking their security controls.



Base: 413 security leaders with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

Cybersecurity Needs To Mature As A Business Strategy

Cybersecurity cannot only be an act of activity-based defense. Today's digital business requires a new way to measure and manage cybersecurity as a strategic business risk. This new approach needs to be focused on both understanding the current risk posture and predicting the greatest threats to the business. These insights empower more informed risk-based decisions and focus security on what matters to the business.

We asked security leaders to rate their security practices across various areas of oversight, technology, process, and people — areas based on a proactive, predictive approach to cyber risk that is aligned to the business.

The study found that security leaders who excel in these areas are much better equipped to speak the language of business risk. These business-aligned security leaders are 8x as likely as their more siloed peers to be highly confident in their ability to answer the question, "How secure, or at risk, are we?"

72%

of business-aligned security leaders are very or completely confident in their ability to report on their organizations' level of risk versus just 9% of their more siloed peers.

OVERSIGHT

- Cybersecurity strategy is developed to support organization strategy with defined metrics to track and improve business alignment.
- Cybersecurity strategy is forward-looking and predictive.
- Security leaders are involved with informing and setting business strategy.
- There are defined metrics and benchmarking processes tied to business performance and process improvement.
- The quantifiable analyses of risk are used to support prioritization and cost justification of mitigation efforts.
- The decision to address a risk is based on maximizing business outcomes within defined risk thresholds.

TECHNOLOGY

- Automated vulnerability management assessments are used with measurements to identify gaps in coverage.
- Key risk and performance metrics are established to maximize business access to data while mitigating risk.
- The security organization has a holistic understanding and assessment of the entire attack surface.
- There is good visibility into the security of the organization's most-critical assets, including IT, OT, and IoT.

PROCESS

- A risk-based approach is used to prioritize and justify mitigation efforts, according to business needs and risk management objectives.
- The monitoring and incorporation of threat intelligence for likelihood of exploitation as well as asset value is automated.
- A combination of asset criticality and vulnerability is used to prioritize remediation.
- Vulnerability assessments are conducted on a frequent basis using automated tools.
- Automated processes exist for applying business risk management objectives to vulnerability prioritization practices.

PEOPLE

- Cybersecurity initiatives are closely aligned with business priorities.
- The security organization works with business stakeholders to align cost, performance, and risk reduction objectives with business needs.
- There is a BISO or similar role who works with each line of business to minimize risk, maximize protection, and increase the value of the organization's business information assets.
- IT operations and the security organization are closely aligned to ensure that the vulnerabilities that pose the greatest risk to the business are remediated quickly and effectively.
- Performance metrics are regularly reviewed with business stakeholders.
- The security organization closely tracks its performance, costs, and risk management efforts.

Note: Representative list of metrics used for assessment
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

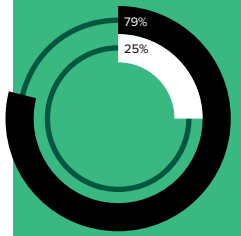
Business-Aligned Security Leaders Manage Cybersecurity As A Strategic Business Risk

So what sets business-aligned security leaders apart from their more reactive and siloed peers? Our study revealed that:

- **BUSINESS-ALIGNED SECURITY LEADERS ARE MORE LIKELY TO ALIGN CYBERSECURITY INITIATIVES WITH BUSINESS OBJECTIVES.**

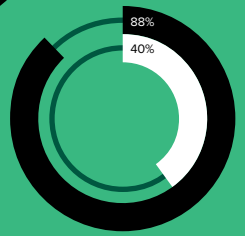
  Business-aligned security leaders ensure their strategies are in lockstep with business priorities. They collaborate with business leaders not only to develop strategies and metrics to support organizational goals but also to inform, set, and make decisions related to business strategies. To that end, eight out of 10 business-aligned security leaders say they have a business information security officer (BISO) or similar executive to ensure each line of business works to minimize risk, maximize protection, and increase the value of the organization's business information assets.

Compared to the more reactive and siloed security leaders, business-aligned security leaders are:



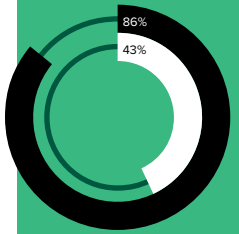
3.2x

more likely to ensure cybersecurity objectives are closely aligned to business priorities.



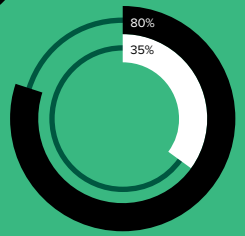
2.2x

more likely to develop and implement cybersecurity strategy to support organizational strategy, with defined metrics to track and improve business alignment.



2x

more likely to be involved in helping inform, set, and make decisions related to the organization's business strategies.



2.3x

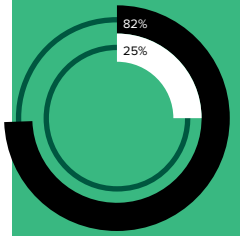
more likely to have a BISO or similar executive who ensures each line-of-business works to minimize risk, maximize protection, and increase the value of the organization's business information assets.

Base: 104 business-aligned and 104 reactive and siloed security leaders
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

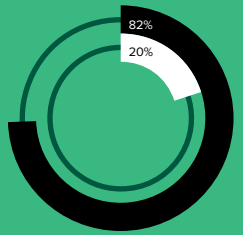
- **BUSINESS-ALIGNED SECURITY LEADERS HAVE A COMPREHENSIVE VIEW OF THEIR ORGANIZATIONS' ATTACK SURFACES AND MOST BUSINESS-CRITICAL ASSETS.**

  It's difficult — if not impossible — to accurately determine the degree to which your organization is secure or at risk without having a full understanding of your attack surface and asset criticality. Business-aligned security leaders not only are far more likely than their more siloed counterparts to have a holistic understanding of their organizations' entire attack surfaces, but they also have better visibility into the security of their most critical assets. This knowledge informs their approaches to remediation, where a combination of asset and vulnerability criticality factors into prioritizing remediation efforts.

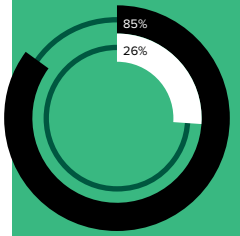
Compared to the more reactive and siloed security leaders, business-aligned security leaders are:



3.3x
more likely to have a holistic understanding and assessment of their organization's entire attack surface.



4.1x
more likely to have good visibility into the state of security of their organization's most critical assets.



3.3x
more likely to use a combination of asset and vulnerability criticality when prioritizing remediation efforts.

Base: 104 business-aligned and 104 reactive and siloed security leaders
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

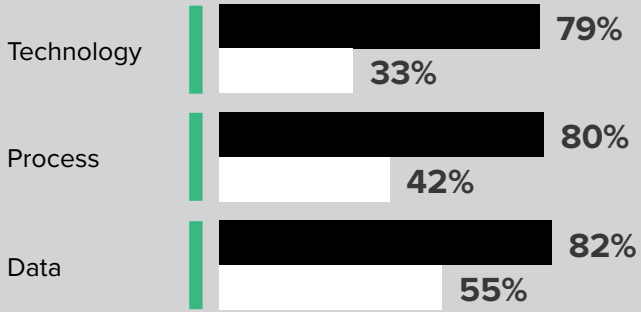
- **BUSINESS-ALIGNED SECURITY LEADERS ARE MORE CONFIDENT THEY HAVE THE NECESSARY RESOURCES TO IDENTIFY AND PREDICT THREATS.**

  Attempting to communicate business risk when you lack confidence in the tools you have at your disposal can be a futile effort. Yet few reactive and siloed security leaders are completely or very confident they have the technology, processes, and data to identify the risk level that cybersecurity threats pose to the business. Conversely, roughly eight in 10 business-aligned leaders are highly confident they are well-equipped across all three of these areas. Similarly, while more than six out of 10 business-aligned security leaders are highly confident they have the technology, processes, and data to accurately predict the likelihood of a cybersecurity threat impacting the business, fewer than half of their more reactive peers can say the same.

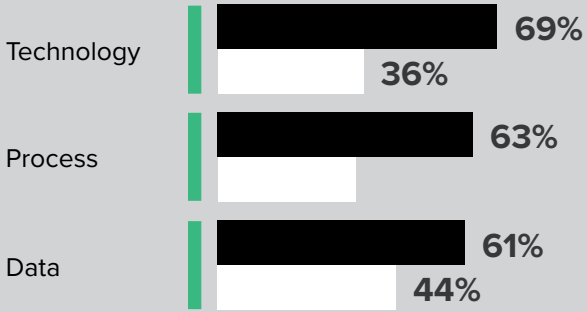
"How confident are you that your security organization has the technologies, processes, and data to accurately . . .?"

- Business-aligned
- Reactive and siloed

IDENTIFY THE RISK LEVEL CYBERSECURITY THREATS POSE TO THE BUSINESS



PREDICT THE LIKELIHOOD OF A CYBERSECURITY THREAT IMPACTING THE BUSINESS

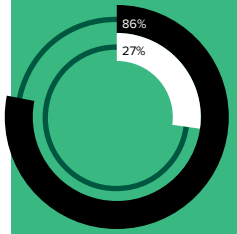


Base: 104 business-aligned and 104 reactive and siloed security leaders
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

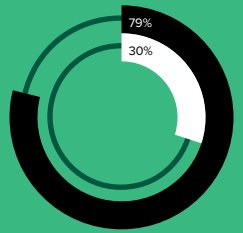
- **BUSINESS-ALIGNED SECURITY LEADERS TAKE A PROACTIVE APPROACH TO VULNERABILITY ASSESSMENT BY AUTOMATING KEY PROCESSES.**

  Malicious actors are continuously finding new ways and opportunities to infiltrate businesses, as illustrated by the wave of COVID-19-related malware and phishing attacks. Security leaders cannot afford to sit back and react to the next attack; they must shift their approaches from reactive to proactive. Business-aligned security leaders outpace their more reactive and siloed counterparts in automating key vulnerability assessment processes by margins of +49 to +66 percentage points.

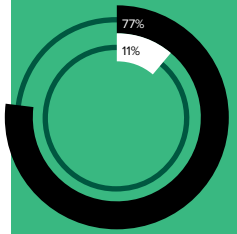
Compared to the more reactive and siloed security leaders, business-aligned security leaders are:



3.2x
more likely to use automated tools to conduct vulnerability assessments on a frequent basis.



2.6x
more likely to automate the monitoring and incorporation of threat intelligence for likelihood of exploitation.



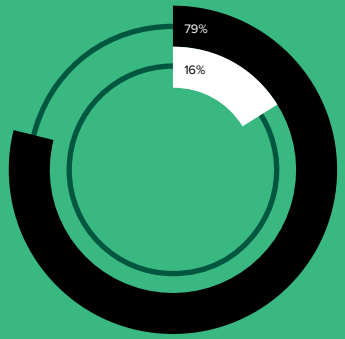
7x
more likely to automate the application of business risk management objectives to vulnerability prioritization practices.

Base: 104 business-aligned and 104 reactive and siloed security leaders
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

- **BUSINESS-ALIGNED SECURITY LEADERS WORK WITH BUSINESS STAKEHOLDERS TO ENSURE CYBERSECURITY OBJECTIVES AND METRICS ALIGN WITH BUSINESS NEED.**

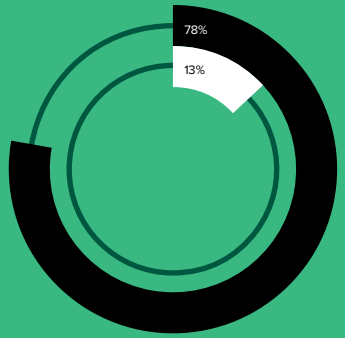
  Cyber risk management has long been measured based on tactical efforts and technical cybersecurity metrics. But to offensively manage cybersecurity risk and drive better decisions, security leaders must standardize on metrics that speak to business risk. Business-aligned security leaders don't define metrics in a vacuum: They are six times as likely to review performance metrics with business stakeholders than their more siloed counterparts. Eight out of 10 say they partner with the business to ensure close alignment on cost, performance, and risk reduction objectives compared to just 16% of their peers.

Compared to the more reactive and siloed security leaders, business-aligned security leaders are:



4.9x

more likely to work with business stakeholders to align cost, performance, and risk reduction objectives with business need.



6x

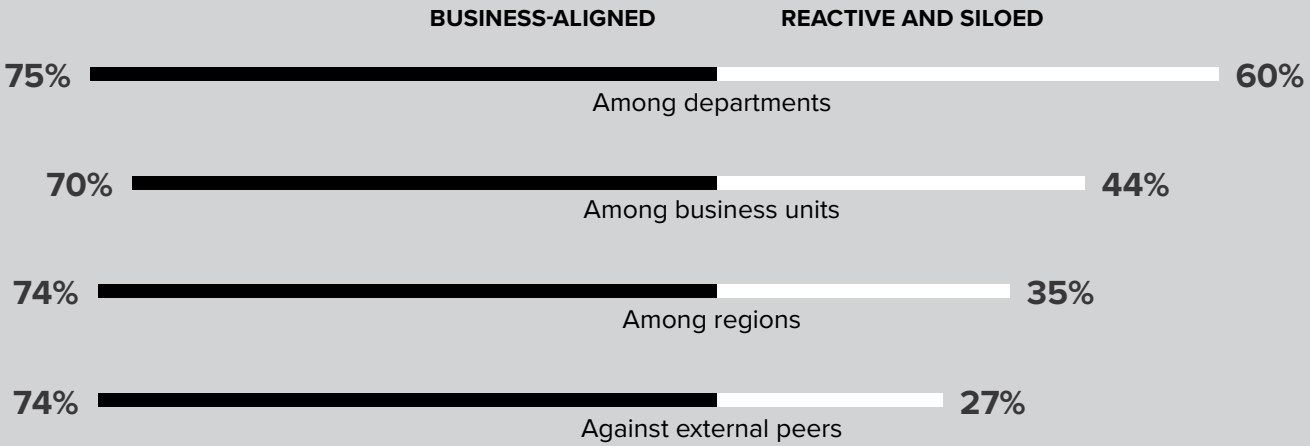
more likely to regularly review security organization performance metrics with business stakeholders.

Note: Percentages reflect a rating of 4 or 5, where 5 is "completely describes my organization"
Base: 104 Business-aligned and 104 Reactive and siloed security leaders
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

- **BUSINESS-ALIGNED SECURITY LEADERS BENCHMARK BOTH THEIR INTERNAL AND EXTERNAL CYBERSECURITY PERFORMANCE.** It's difficult to gauge the maturity of your cybersecurity program if you aren't benchmarking it both internally and against external peers. Business-aligned security leaders are more likely than their more reactive counterparts to have a defined benchmarking process: 86% have a process that clearly articulates expectations and demonstrates continuous process improvement relative to peer companies and/or internal groups, compared with just 32% of their reactive and siloed peers. This results in stronger internal and external cybersecurity benchmarking capabilities: Business-aligned security leaders outpace more reactive leaders by margins of +15 to +47 percentage points.

"Please rate your security organization's ability to benchmark cybersecurity practices internally and externally."

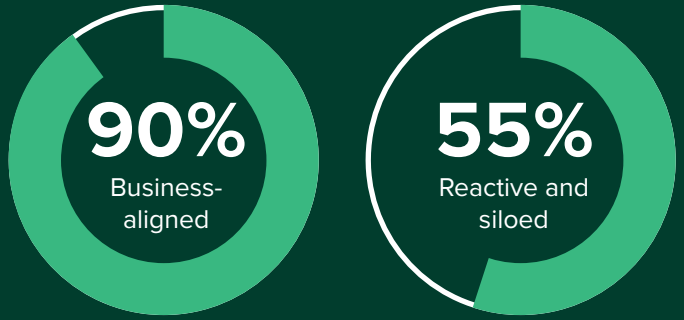
(Showing good or excellent responses)



Base: 104 business-aligned and 104 reactive and siloed security leaders
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

- **BUSINESS-ALIGNED SECURITY LEADERS DEMONSTRATE THE VALUE OF THEIR CYBERSECURITY INVESTMENTS.**
  In this unprecedented climate of economic uncertainty, security leaders must also be ready to demonstrate the impact of cybersecurity investments. Strategies and practices built around understanding business risk give business-aligned leaders confidence in their ability to demonstrate the impact of cybersecurity investments. Most business-aligned security leaders are very or completely confident in their ability to demonstrate that their cybersecurity investments are positively impacting their business performance compared with just over half of their more reactive and siloed counterparts. This confidence is, in part, rooted in their use of metrics to track cybersecurity ROI and impact on business performance.

"How confident are you in your ability to demonstrate that your organization's cybersecurity investments are positively impacting your organizational/business performance?"
(Showing very or completely confident responses)



85%
of business-aligned security leaders have metrics to track cybersecurity ROI and impact on business performance versus just 25% of their more reactive and siloed peers.*

*Note: A rating of 4 or 5, where 5 is "completely describes my organization"
Base: 104 business-aligned and 104 reactive and siloed security leaders
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

Recommendations

Modern security threats require a new approach. Security leaders must align their cybersecurity strategies with business objectives and priorities to evolve from the old reactive and siloed approach of "detect, protect, and defend" to a strategy that empowers security and the business to take an offensive view of cybersecurity risk and align it to business decisions. Managing cybersecurity as a business risk requires that security leaders:

Communicate clearly and with confidence.

A whopping 66% of business leaders are — at most — only somewhat confident in their security teams' ability to quantify their organizations' level of risk or security. However, business-aligned security leaders are **eight times** more likely than their siloed counterparts to be highly confident in their ability to answer the question, "How secure, or at risk, are we?"

Align cybersecurity initiatives with business objectives.

Enlist a BISO or equivalent executive in collaborating with the leaders of each line of business to develop strategies, goals, and metrics to maximize the protection of business information assets. Organizations that have tight alignment between business and security are **2.3 times** more likely to have a BISO or similar executive.

> **"[Security leaders] need a translator — someone that understands the goals of the business and also understands security and how to pivot in a way that prioritizes internal education around how to translate value."**
>
> — Business information security officer, financial services

Benchmark both internal and external relative cybersecurity performance.

Articulate expectations about cybersecurity performance and demonstrate continuous process improvement relative to both peer companies and internal groups. A limited approach to benchmarking makes it difficult to gauge cybersecurity performance. Business-aligned security leaders are more likely than their more reactive counterparts to have a defined benchmarking process: **86% have a process** that clearly articulates expectations and demonstrates continuous process improvement relative to peer companies and/or internal groups, compared with just 32% of their peers.

> **"What you might typically see as corporate objectives on growth, customer retention, satisfaction, and the like — even though those objectives are not necessarily security objectives — there's usually a way to align what you want to do with one of those objectives."**
>
> — VP and chief information security officer, business process outsourcing and human capital management

Prioritize vulnerability assessment by automating key processes.

Prioritization based on business risk context will help focus your efforts. You can accomplish this by automating vulnerability assessment processes — including monitoring and incorporating threat intelligence and applying business risk management objectives to vulnerability prioritization practices utilizing a predictive approach — and by conducting vulnerability assessments on a frequent basis using automated tools. Business-aligned security leaders are **3.3 times** more likely to use a combination of asset criticality and vulnerability factors when prioritizing remediation efforts. Such leaders are also **seven times** more likely to automate the application of business risk management objectives to vulnerability prioritization practices.

Develop a comprehensive assessment of the organization's most business-critical assets.

A robust prioritization strategy for business impact mitigation requires a holistic understanding of the organization's entire attack surface, including remote workers, OT, and cloud deployments, as well as insight into which assets pose the greatest business risk if compromised. Business-aligned security leaders are **3.3 times** more likely than their more siloed counterparts to have a holistic understanding of their organizations' entire attack surfaces.

Define metrics to demonstrate the value of cybersecurity investments.

Few security organizations use threat metrics that speak to business risk. At the heart of the issue is a lack of partnership between security and business leaders to ensure alignment between cybersecurity metrics and objectives with business priorities. Gain confidence to demonstrate the value of cybersecurity investments to business leaders by cultivating and consuming cybersecurity metrics for both ROI and the impact on business performance. Business-aligned security leaders don't define metrics in a vacuum: They are **six times** as likely to review performance metrics with business stakeholders than their more siloed counterparts. **Eight out of 10** say they partner with the business to ensure close alignment on cost, performance, and risk reduction objectives compared to just 16% of their peers. And 85% of business-aligned security leaders have metrics to track cybersecurity ROI and impact on business performance versus just 25% of their more reactive and siloed peers.

Project Director:

Heather Vallis, Principal Market Impact Consultant & Manager

Contributing Research:

Forrester's Security & Risk research group

Methodology

In this study, Forrester conducted an online survey of 416 security and 425 business executives, as well as telephonic interviews with five business and security executives, to examine cybersecurity strategies and practices at midsize to large enterprises in the US, the UK, Germany, France, Australia, Mexico, India, Brazil, Japan, and Saudi Arabia. The study was fielded in April 2020.

Demographics

NUMBER OF EMPLOYEES

- 12% 20,000 or more
- 26% 5,000 to 19,999
- 51% 1,000 to 4,999
- 12% 500 to 999

JOB LEVEL: SECURITY

- 18% Senior-most IT or security decision maker
- 27% VP in IT or security
- 55% Director

ROLE

- 49% Security
- 51% Business

JOB LEVEL: BUSINESS

- 18% Senior-most business leader
- 20% Senior risk/compliance leader
- 49% Executive in line of business or function
- 13% Board member

Note: Percentages may not total 100 because of rounding
Base: 416 security and 425 business executives with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Additional data

"How many times did your organization experience a business-impacting cyberattack or compromise within the past 12 months?"

	AUSTRALIA (N = 105)	BRAZIL (N = 59)	FRANCE (N = 104)	GERMANY (N = 103)	INDIA (N = 54)	JAPAN (N = 51)	MEXICO (N = 104)	SAUDI ARABIA (N = 52)	UNITED KINGDOM (N = 103)	UNITED STATES (N = 106)
NONE	5%	2%	5%	1%	2%	0%`	2%	4%	3%	1%
1	3%	5%	1%	3%	6%	2%	1%	0%	3%	2%
2	6%	3%	5%	2%	6%	6%	4%	8%	8%	4%
3	10%	10%	17%	11%	24%	18%	15%	10%	16%	21%
4	18%	39%	27%	33%	24%	18%	28%	33%	22%	25%
5 OR MORE	55%	39%	40%	47%	37%	55%	47%	44%	47%	44%
DON'T KNOW	4%	2%	5%	4%	2%	2%	3%	2%	2%	3%

Note: Percentages may not add to 100% due to rounding
Base: Varies; security leaders and business executives with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

Additional data

"Did any of these business-impacting cyberattacks or compromises involve your organization's operational technology systems?"

	AUSTRALIA (N = 96)	BRAZIL (N = 57)	FRANCE (N = 94)	GERMANY (N = 98)	INDIA (N = 52)	JAPAN (N = 50)	MEXICO (N = 99)	SAUDI ARABIA (N = 49)	UNITED KINGDOM (N = 98)	UNITED STATES (N = 102)
YES	73%	53%	64%	61%	67%	68%	67%	61%	65%	65%
NO	27%	47%	36%	38%	33%	32%	32%	39%	34%	33%
DON'T KNOW	0%	0%	0%	1%	0%	0%	1%	0%	1%	2%

Base: Varies; security and business leaders at organizations experiencing a business-impacting cyberattack or compromise within the past 12 months
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

Additional data

"How confident are you in your security organization's ability to answer the question, 'How secure, or at risk, are we?' at any given time for your business?"

	AUSTRALIA (N = 105)	BRAZIL (N = 59)	FRANCE (N = 104)	GERMANY (N = 103)	INDIA (N = 54)	JAPAN (N = 51)	MEXICO (N = 104)	SAUDI ARABIA (N = 52)	UNITED KINGDOM (N = 103)	UNITED STATES (N = 106)
VERY/ COMPLETELY CONFIDENT	28%	36%	43%	33%	37%	38%	46%	43%	40%	36%
SOMEWHAT CONFIDENT	50%	34%	33%	35%	33%	41%	29%	33%	39%	42%
NOT THAT/ NOT AT ALL CONFIDENT	23%	30%	24%	32%	30%	22%	26%	25%	21%	21%

Note: Percentages may not add to 100% due to rounding
Base: Varies; security leaders and business executives with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

"How did this/these attack(s) or compromise(s) impact your organization?"

(Select all that apply)

	AUSTRALIA (N = 96)	BRAZIL (N = 57)	FRANCE (N = 94)	GERMANY (N = 98)	INDIA (N = 52)	JAPAN (N = 50)	MEXICO (N = 99)	SAUDI ARABIA (N = 49)	UNITED KINGDOM (N = 98)	UNITED STATES (N = 102)
LOSS OF CUSTOMER DATA	39%	33%	33%	37%	38%	38%	25%	41%	34%	48%
LOSS OF EMPLOYEE DATA	36%	32%	32%	35%	38%	32%	28%	41%	44%	44%
LOSS OF PRODUCTIVITY	39%	46%	38%	45%	31%	30%	47%	18%	26%	27%
FINANCIAL LOSS OR THEFT	39%	33%	31%	35%	38%	46%	27%	35%	36%	35%
IDENTITY THEFT	30%	26%	28%	36%	44%	44%	29%	24%	23%	39%
COMPROMISE OF OTHER CONFIDENTIAL DATA	36%	25%	24%	33%	19%	42%	29%	35%	34%	35%
NETWORK/BUSINESS APPLICATIONS UNAVAILABLE	33%	35%	27%	33%	23%	36%	21%	31%	23%	33%
CUSTOMER ATTRITION	29%	32%	22%	31%	33%	32%	18%	33%	34%	31%
THEFT OF INTELLECTUAL PROPERTY	27%	26%	30%	31%	29%	40%	20%	33%	23%	24%
DAMAGE TO BRAND/REPUTATION	27%	12%	29%	30%	25%	32%	20%	31%	24%	26%
RANSOMWARE PAYOUT	32%	14%	26%	22%	33%	34%	17%	37%	22%	22%
REGULATORY FINES	22%	19%	27%	23%	25%	32%	20%	31%	23%	29%
SYSTEM DESTRUCTION/PHYSICAL DAMAGE	27%	12%	24%	20%	21%	34%	24%	27%	27%	26%
INCREASED EMPLOYEE TURNOVER	28%	23%	23%	27%	23%	42%	18%	27%	18%	22%
MISSED REVENUE GOALS	28%	12%	22%	23%	17%	30%	17%	27%	22%	32%
LEGAL LIABILITY	27%	12%	30%	21%	25%	20%	20%	16%	27%	26%
DECLINE IN STOCK PRICE	21%	14%	21%	17%	12%	46%	22%	22%	18%	25%
NO IMPACT	2%	2%	4%	3%	0%	0%	0%	0%	1%	0%

Note: Percentages may not add to 100% due to rounding Base: Varies; security and business leaders at organizations experiencing a business-impacting cyberattack or compromise within the past 12 months
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

Additional data

"Has the number of business-impacting cyberattacks increased compared with 24 months ago?"
(Increased somewhat or significantly)

"Do you expect the number of business-impacting cyberattacks will increase over the next 24 months?"
(Will increase somewhat or significantly)

	AUSTRALIA (N = 105)	BRAZIL (N = 59)	FRANCE (N = 104)	GERMANY (N = 103)	INDIA (N = 54)	JAPAN (N = 51)	MEXICO (N = 104)	SAUDI ARABIA (N = 52)	UNITED KINGDOM (N = 103)	UNITED STATES (N = 106)
INCREASED COMPARED WITH 24 MONTHS AGO	73%	67%	64%	74%	76%	81%	54%	85%	63%	67%
EXPECT AN INCREASE OVER THE NEXT 24 MONTHS	76%	83%	69%	83%	74%	84%	74%	81%	78%	78%

Base: Varies; security leaders and business executives with responsibility over cybersecurity/security strategies and budgets
Source: A commissioned study conducted by Forrester Consulting on behalf of Tenable, April 2020

FORRESTER®