A Forrester Consulting
Thought Leadership Paper
Commissioned By BMC

July 2020

A False Sense Of Mainframe Security

How Overconfidence And Complacency Leave Companies Vulnerable To Attack

FORRESTER®

Table Of Contents

Project Director:
Emily Drinkwater,
Market Impact Consultant

Contributing Research:
Forrester’s Security & Risk
research group

FORRESTER®

Organizations are often mistaken to believe that "secure" is inherent for mainframes. In reality, secure means "securable."

Executive Summary

Mainframes are often considered one of the most secure data environments, but organizations are mistaken to believe that mainframes are inherently secure. In reality, secure means "securable." In this research, we explored the current perceptions of mainframe security, the readiness of companies to prepare and secure the mainframe for a modern enterprise, and the benefits of having a more secure mainframe.

BMC commissioned Forrester Consulting to evaluate the tools, actions, and maturity of mainframe security in enterprises. Forrester surveyed 264 security decision makers in North America and EMEA with insights into mainframe security at enterprises across all industries to evaluate mainframe security practices and perceptions. We also conducted 4 qualitative interviews within the same demographic. We found that while some enterprises embrace mainframe security as a top priority, there are many who have work to do to properly secure their mainframe.

KEY FINDINGS

- **Only 41% are taking the steps needed to actively secure the mainframe.** This is because IT leaders are more focused on network and vendor security and often confuse "secure" and "securable" for mainframes. Although the natural architecture of a mainframe lends itself to be more isolated from public attacks, it is not immune to threats. Plus, any attack on an external system will trickle down to the mainframe. Just because a mainframe is readily securable does not mean it is inherently already secure.
- **Over 80% said they have the right tools but still experience major security events.** Mainframe challenges are even more exacerbated for organizations with less mature mainframe security tactics. Organizations are plagued with mainframe tools that do not meet their needs, negative perceptions to battle, and major gaps in the talent pool. Many look to managed services to fill these gaps.
- **Mainframe security maturity drives clear benefits of reduced risk (63%) and increased efficiency (64%).** By having a more secure mainframe and an active security approach, organizations can unlock the key benefits they need the most: reduced risk and increased efficiency. More mature organizations also complete the mainframe vulnerability management lifecycle in half the time of less mature organizations.

IT Leaders Confuse “Secure” And “Securable” For Mainframes

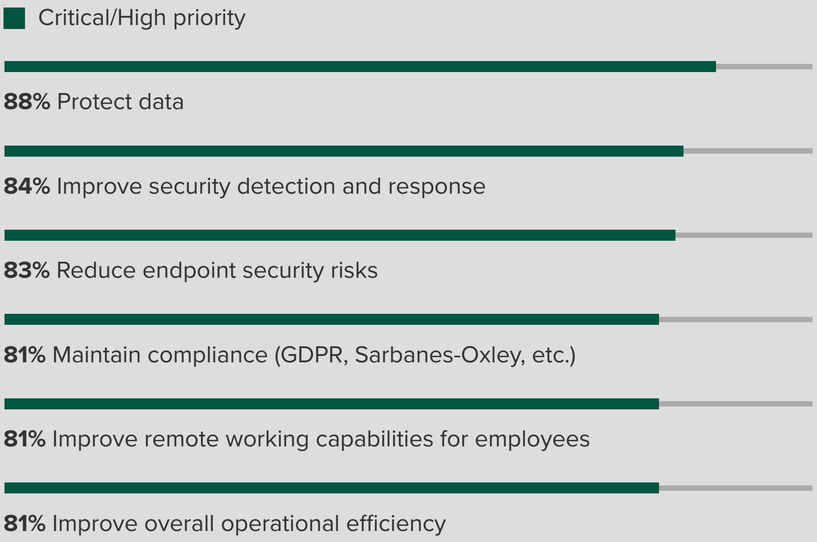
Security, data management, and risk reduction are top of mind in IT organizations, regardless of their view of the mainframe. However, mainframes can be the key to unlocking data security and risk reduction in a modern enterprise if the right approach is taken. In surveying 264 decision makers across industries, we found that:

- **Data protection and risk reduction are top IT priorities.** In a typical IT environment, top priorities often include reducing risk and increasing security measures, as is the case with these organizations (see Figure 1). However, now that we are in an atypical environment in light of the COVID-19 pandemic, many of these priorities are more important than ever before. Respondents said improved security detection and response (59%), protecting data (58%), and reducing endpoint security risks (55%) has increased in priority for their organization due to COVID-19. For many, this means that new initiatives may be on hold while companies go back to the basics of improving security across the board. A CISO and VP at a financial technology company noted:

> *“Because of COVID-19, our primary priority, at least for the next six months or so, is improving work-from-home security. Our workforce has moved from 3% work from home to 97% work from home.”*

Figure 1: Top IT Priorities For Next 12 Months

“How important are the following IT priorities to your organization over the next 12 months?” (Top 6 of 12 shown)



Base: 264 security decision makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

Because of COVID-19, security detection and response (59%), protecting data (58%), and reducing endpoint security risks (55%) has increased in priority for organizations.

- **The theme of risk reduction and improved security continues for mainframe priorities.** With COVID-19 and "business as unusual" in mind, it comes as no surprise that firms are most concerned with securing their mainframes against threats and streamlining capabilities through improved availability and automation. IT leaders cited their top mainframe priorities for the next 12 months as:
  - Increasing security for the mainframe (61%).
  - Identifying and preventing data breaches (52%).
  - Increasing application availability and automating mainframe operations (48%).
  - Maintaining identity access management (47%).
- **IT leaders see mainframes as one of the most secure environments in their organization.** In looking at a list of various environments within an organization, 82% said that the mainframe is very or extremely secure, ranking it near the top of the list (see Figure 2). In fact, they ranked all internal environments within their control near the top, while public environments that are out of their control, such as public cloud servers, fall to the bottom of the list.

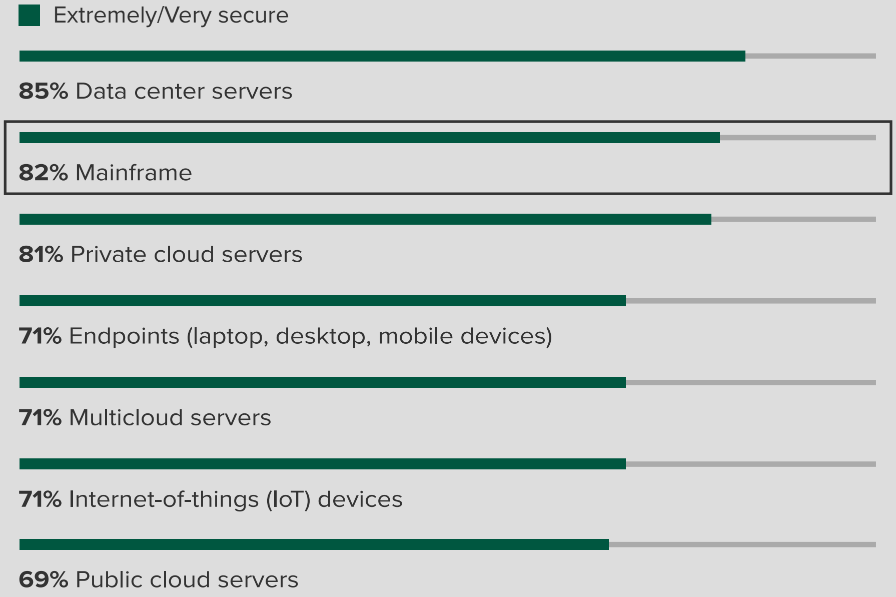
  Members of the IT C-suite noted that although mainframe architecture lends itself to more inherent security, that isn't to say that it cannot be compromised:

> "The mainframe platform, by design, is very secure. It's very different from a server sitting in public, unlike the mainframe that's not in a high-risk area."
>
> ***CISO and VP at a financial technology company***

> "I think mainframes are inherently more secure just because of the architecture and whatnot, and they are more securable. . . . That isn't to say they can't be hacked. Anything can be hacked."
>
> ***Chief of mainframe systems at federal government department***

Figure 2: Ranking Of Secure Environments

"At your organization, how secure do you perceive the following environments to be?"



Base: 264 security decision makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

- **Many believe the mainframe is inherently secure, although they have no active security efforts to support their belief.** This is indicative of a much larger issue of mainframe security perception that many professionals confuse "secure" with "securable." Due to the belief that mainframes are one of the most secure environments, only 41% are taking the steps needed to actively secure the mainframe by treating the mainframe like any network, internet-connected device. The attitude of this professional unfortunately sums up the attitude of many:

> *"It's not public facing, and it takes a specialized skillset to compromise a mainframe."*
>
> ***CISO and VP at a financial technology company***

Only 2 in 5 are taking the steps needed to actively secure the mainframe.

AN ANALYSIS OF MAINFRAME SECURITY READINESS AT ORGANIZATIONS

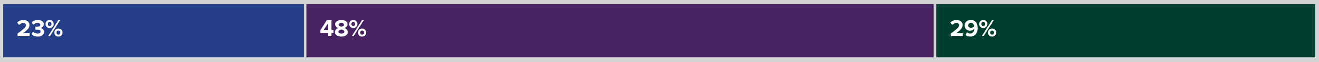
While many organizations view the mainframe as a secure platform, few are taking the steps required to actually secure the mainframe. This research explored the readiness of organizations to prepare and secure the mainframe for the modern IT enterprise. In order to determine an organization's readiness, we asked respondents a series of questions and scored their responses to place them on a readiness curve.[1] These questions included their perception of mainframe security, their organization's attitude toward mainframe security, mainframe security risks their organization experienced, and the level of screening/visibility/security features in place. The scales for each question were ranked by least ready (1) to most ready (5). The sum of these values indicates the mainframe security readiness score of each respondent. Respondents were grouped into three tiers based on their aggregate scores: Not Ready, Complacent, and Ready.

In an examination of the mainframe security readiness groups, we determined the following key characteristics of each group (see Figure 3).

While many organizations view the mainframe as a secure platform, few are taking the steps required to actually secure the mainframe.

Figure 3: Mainframe Security Readiness Scores

Not Ready	Complacent	Ready
(Avg score = 1.0 to 3.4) N = 61	(Avg score = 3.5 to 4.0) N = 127	(Avg score = 4.1 to 5.0) N = 76



Top 3 Industries

Not Ready	Complacent	Ready
18% Financial services/insurance	**20%** Technology/tech services	**20%** Technology/tech services
16% Technology/tech services	**16%** Financial services/insurance	**13%** Financial services/insurance
13% Manufacturing and materials	**8%** Healthcare	**11%** Manufacturing and materials
		11% Retail (Tie)

Key Characteristics

Not Ready	Complacent	Ready
Thinks ID access management is enough to secure the mainframe, mainframe security is purely an administrative function based on authentication and authorization, or gives other environments a higher priority	Actively works to meet mainframe compliance standards, but mainframe security isn't a top priority	Secures the mainframe like any network, internet-connected device
Does not have the tools required to know if someone gained unauthenticated access, had elevated privileges, or unsecured data	Has experienced someone gaining unauthenticated access, getting elevated privileges, or having unsecured data, but had the tools to uncover the issues	Has not experienced someone gaining unauthenticated access, getting elevated privileges, or having unsecured data, but had the tools to uncover the issues
Is not confident in mainframe visibility and security procedures	Is moderately confident in mainframe visibility and security procedures	Is very confident in mainframe visibility and security procedures

Vulnerability Lifecycle Management

Average number of business days to complete the vulnerability management lifecycle:

Not Ready	Complacent	Ready
41.7 Business days	44.6 Business days	20.0 Business days

Base: 264 security decision makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

Mainframe Challenges Are Exacerbated For Organizations With Less Mature Mainframe Security Tactics

The lack of mainframe security readiness that is rampant among organizations as they prepare for a modern IT enterprise only exacerbates challenges that many face in their mainframe environments. In an analysis of mainframe challenges, we found that:

- **Mainframe security is often not a priority due to perceived security elsewhere.** Those who are in the Not Ready group said they are not actively securing their mainframe because they think perimeter network security (36%) and vendor security capabilities (36%) are sufficient. So their focus is directed elsewhere, such as securing newer cloud-based technologies (42%).

  However, more mature mainframe professionals see this as an issue because security is not inherent:

Many don't actively secure the mainframe because they think perimeter network security and vendor security capabilities are sufficient.

> "If you don't secure the distributed platforms, you are exposing yourself to risk. You can't secure one platform over the other because they are all connected. If there is a breach or weak spot anywhere, it will all trickle down to the mainframe."
>
> ***Manager of mainframe computer operations at a transportation/ logistics company***

"If there is a breach or weak spot anywhere, it will all trickle down to the mainframe."

> "Our security modernization effort is focused all across the board. Some people are much more focused on one area — like cloud — than other areas — like mainframes — because they think a hack is less likely. But our concern is equal. We do not believe in security through obscurity."
>
> ***Manager of mainframe computer operations at a transportation/ logistics company***

"We do not believe in security through obscurity."

- **Companies are overconfident in their mainframe tools.** Eighty-two percent of IT leaders said that they can easily find the right mainframe tools. However, of those who said they can find the right tools, they still find the following mainframe tasks very or extremely challenging:
  - Protecting systems from cyberattacks (61%).
  - Quickly identifying vulnerabilities in the operating system (60%).
  - Quickly identifying vulnerabilities in apps (57%).
  - Unifying controls under a single set of recourses (57%).

  If these common mainframe tasks are still incredibly challenging with the "right" tools, then perhaps the right tools aren't in use at all!

- **Personnel challenges plague teams, so many look to managed services.** It is very difficult for companies to find qualified mainframe personnel. Sixty-nine percent claimed to be understaffed and 69% are struggling for talent gaps in the workforce (see Figure 4). Those who are understaffed said that, on average, they are understaffed by 32%. The manager of mainframe computer operations at a transportation/ logistics company said:

  > *"Finding the right personnel in the marketplace to come in, blend in, and adapt right now is really tough."*

  While the talent gaps push many to train from within or reskill employees, 84% find value in looking to managed services providers to help fill those gaps and manage mainframe cybersecurity.

84% look to managed services to help manage mainframe cybersecurity.

Figure 4: Mainframe Personnel Challenges

Understaffing/Talent Gaps

69%
Our mainframe cybersecurity team is **understaffed**.

69%
There are **major talent gaps** in the workforce for skilled mainframe cybersecurity personnel.

Training And Reskilling

84%
We have the **resources required to train** our staff on mainframe cybersecurity.

77%
It is **easier to reskill existing employees** on mainframe cybersecurity than it is to hire new personnel.

Managed Services

84%
We **look to managed services** to help us manage our mainframe cybersecurity.

Base: 264 security decision makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

- **Perceptions of mainframes as being antiquated contribute to the lack of modernization.** The unfortunate perception that mainframes are antiquated and outdated add to the struggles that many IT leaders face when lobbying for increased security and attention to the mainframe. C-suite professionals shared many of the perceptions that they battle regularly:

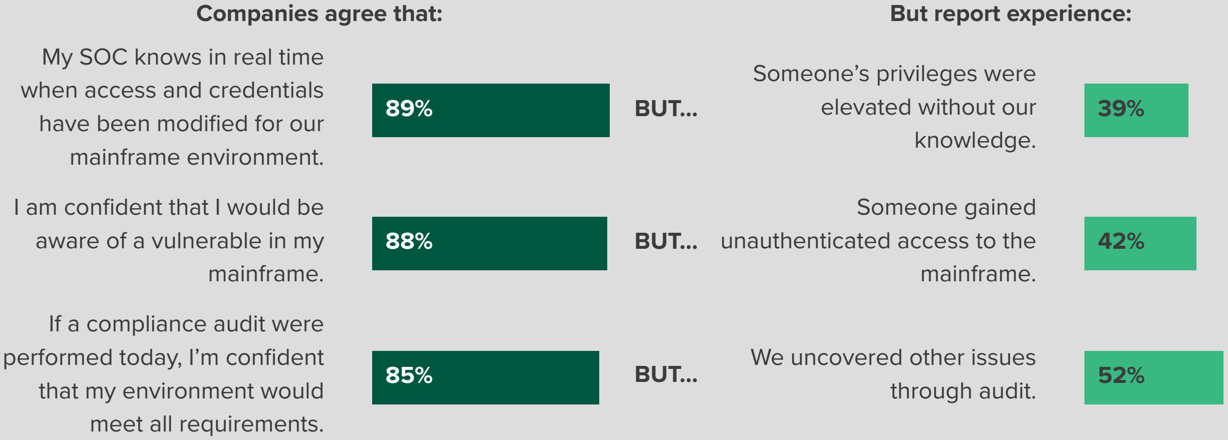
> "They say, 'It's old', 'It's antiquated', and 'I've got to modernize.' Well, you know modernization is not the platform you're on, it's the application you are using. I don't care what platform you are using. Modernization is not the platform itself. People want to blame the platform they are on, but they are often frustrated with the application on the mainframe and confuse the two."
>
> ***Chief of mainframe systems at federal government department***

> "A lot of corporations think mainframes don't have modern capabilities, but mainframes have evolved dramatically. I have been in the mainframe world for decades, and I have seen it evolve."
>
> ***Manager of mainframe computer operations at a transportation/ logistics company***

> "People say mainframes are legacy. Mainframes aren't legacy. They are continually modernized. It's the applications that run on them that are legacy."
>
> ***Enterprise computing vice president at an insurance organization***

- **Security events are still commonplace in mainframes, with 52% of respondents still uncovering issues through audit.** Despite the confidence in mainframes as a secure platform, many respondents said their organizations still experience major security events due to the lack of security measures taken to secure the mainframe. Respondents said they have the skills and tools in place to identify and detect issues, yet they have still experienced significant security compromises (see figure 5). For example, 89% said their security operation center (SOC) knows when credentials are modified, but 39% have still experienced someone's credentials being elevated without their knowledge. Another 85% are confident that an audit would show their environment meets all requirements, but more than half (52%) said they uncover issues through their auditing processes. These security events indicate that perhaps companies should not be quite as confident in the procedures they currently have in place.

Figure 5: Mainframe Security Events



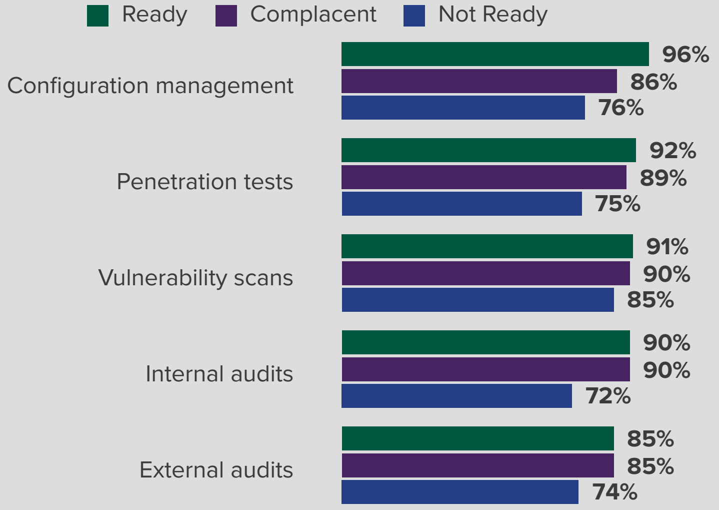
Base: 264 security decision makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

- **More frequent performance of key security tasks is a key indicator of mainframe security maturity.** To properly prepare the mainframe for the modern enterprise, it is critical that organizations regularly perform critical mainframe security tasks such as penetration testing, vulnerability scanning, and configuration management. The Ready organizations are performing key security tasks more often than the Complacent and Not Ready groups, but the definitions of "sometimes" and "regularly" vary widely. Although many in the Complacent and Not Ready groups claim to perform these tasks sometimes or regularly, when asked just exactly how often that is, they indicated that it is much less frequent than the Ready group that performs most of the tasks at least monthly or quarterly. The standards of the Not Ready and Complacent groups indicate a lackluster "good enough" approach to critical mainframe security tasks.

Figure 6: Mainframe Testing Frequency

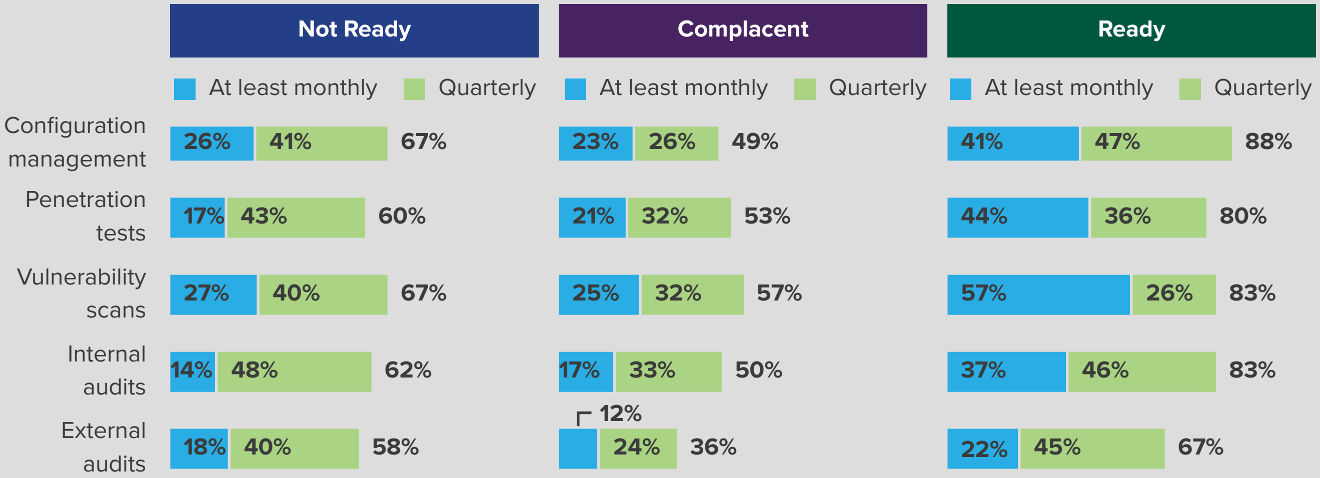
"How often does your organization perform the following security tasks to secure the mainframe?"

(% Sometimes and Regularly shown)



Base: 264 security decision makers in North America and EMEA with insights into mainframe security

"You indicated that you perform the following tasks sometimes or regularly. How often do you perform these tasks?"



Base: Variable security decision makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

For example, the enterprise computing vice president at an insurance organization said that having a central system where all testing and auditing takes place is critical to uncovering key security issues. When asked if he would be aware of unauthorized users on the mainframe, he said:

> *"Yes and no. Yes, we could find out after the fact. But everything is sort of dispersed, and we don't have a central system where all security alerts are reported, which makes it a challenge. We are capable of getting that information with time. It just isn't streamlined yet. That's part of the maturity process we are going through."*

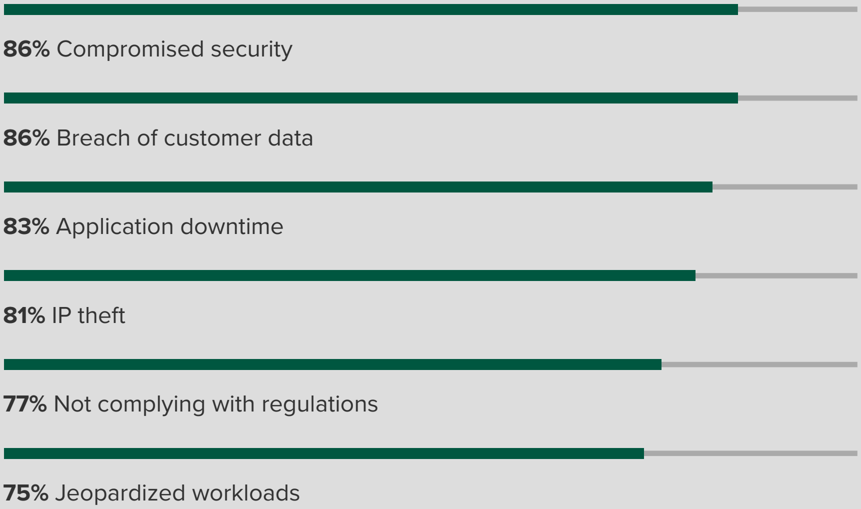
The regular performance of key mainframe security audits, as well as a centralized way to process and report, is a sign of maturity that the Ready group possesses, but that the other groups need to improve in order to mature.

- **The impacts of compromised mainframe security would be devastating, with more than four in five respondents expressing significant concern if the security was compromised.** Even though many are complacent or not taking the steps needed to secure the mainframe, professionals agree that compromised security could be devastating (see Figure 7). Even though their overconfidence means they don't anticipate a breach in security, most mainframe professionals would be moderately or highly concerned if there was compromised security (86%) or a breach of customer data (86%) due to the amount and types of sensitive data stored on the mainframe.

The impacts of compromised mainframe security would be devastating.

Figure 7: Ramifications Of Compromised Mainframe Security

"What is your level of concern with the following ramifications of compromised mainframe security?"
(% Moderate/High concern shown)



Base: 264 security decision makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

Other seasoned mainframe professionals reiterated this:

> "Some databases can take weeks and weeks to recover. You'd be really lucky if you could recover everything."
>
> ***Manager of mainframe computer operations at a transportation/ logistics company***

> "We pride ourselves on securing our platforms, and the mainframe is one of our most critical platforms. Unauthorized access would absolutely be significant. We also pride ourselves on our good reputation, which is key to our business. Our customers expect a level of security and control from us, and we have made a significant investment in security overall — multibillion-dollar investments year over year — to keep up with the increased cyber threats."
>
> ***Enterprise computing vice president at an insurance organization***

"The mainframe is one of our most critical platforms. Unauthorized access would absolutely be significant."

> "Let me put it this way: I've got something like $300 billion to $400 billion worth of transactions that are processed on the mainframe in one of our programs alone — not to mention all of the other programs we operate. We have all of the personally identifiable information (PII) tied to citizens, loans, etc. If someone got in and no one knew they were there, money would disappear. This is all money that a lot of citizens count on and need. We've got a lot of US citizens who would have a potential direct impact of not a friendly kind."
>
> ***Chief of mainframe systems at federal government department***

"We've got a lot of US citizens who would have a potential direct impact [as the result of a mainframe breach]."

- **Overconfidence in mainframe security overlooks one critical component of security: internal threats.** Some of the biggest mainframe threats are internal. Given that the mainframe architecture is inherently isolated from the public for the most part, the majority of IT professionals feel pretty confident (whether justified or not) that they can isolate or prevent mainframe data breaches from external attackers. Although external threats are not impossible and seemingly detrimental, professionals indicated that internal threats are their biggest concern, they could be the most detrimental, and they are the most difficult to protect against and uncover. Mainframe decision makers noted:

Some of the biggest mainframe threats are internal threats.

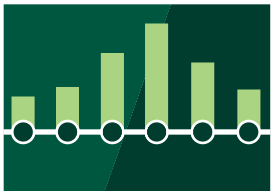
> "I don't inherently feel at risk from an external source coming in and somehow creating or elevating a user's credentials and then just start going after it. I feel pretty comfortable that we'd be able to catch them. . . . But you always have the insider issue that you can't really fix other than through process and trust. For example, say I've got a rogue security officer. They could elevate somebody's privileges because they're a security officer and they have authorization to do that, but it would be an unauthorized elevation. So you wouldn't catch that one per se unless you had another tool that monitors when those changes occur and a different audit process that goes through to make sure that there isn't a rogue agent out there."
>
> ***Chief of mainframe systems at federal government department***

> "Think about the internal threats. You've got to think about the user who may work on my team and may not be having a good day or may have received bad news; they can intentionally or unintentionally sabotage a task or a database."
>
> ***Enterprise computing vice president at an insurance organization***

> "One of the weaknesses of having a centralized security administration group is that you're relying on them to ensure that permissions or entitlements are correctly administered. But who watches the watchers? We have a secondary reviewer who is essentially just a person within the same administration team who reviews the activities of the other one. It helps, but it doesn't eliminate the possibility of collusion."
>
> ***CISO and VP at a financial technology company***

"Who watches the watchers?"

Mainframe Security Maturity Drives Clear Benefits

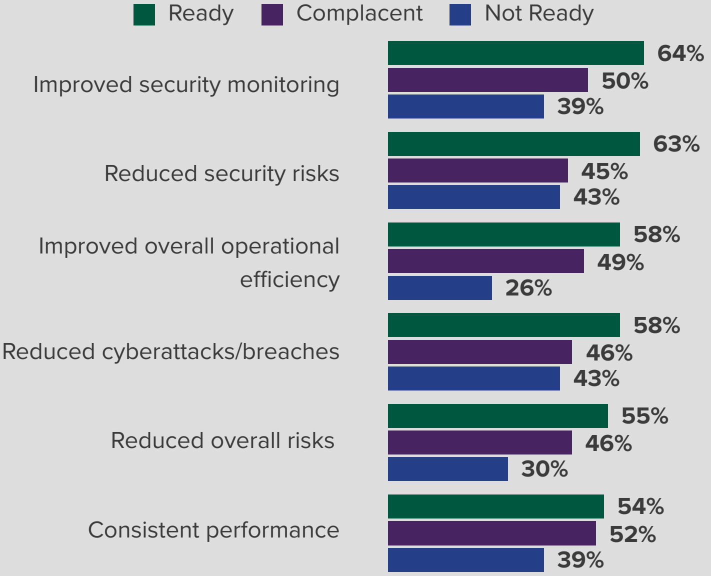


Those in the Ready group who actively work to secure the mainframe experience the benefits that many IT organizations are looking to accomplish. By analyzing the benefits of having a more secure mainframe, we found that:

- **A more secure mainframe improves efficiency (64%) and reduces risks (63%).** These benefits that respondents indicated in their top priorities for the year as critical to their business can be accomplished by taking a more active stance on mainframe security. Those in the Ready group experience significantly more (sometimes twice as much) of the incredible benefits that the mainframe can provide, including reduced risk, reduced cyberattacks, and improved overall operational efficiency (see Figure 8).

Figure 8: Top Benefits Of A More Secure Mainframe

"What benefits have you seen/would you expect from having a secure mainframe?"



Base: 264 security decision makers in North America and EMEA with insights into mainframe security

Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

Those in the Ready group experience significantly more of the benefits that the mainframe can provide.

- **Mature organizations can complete the mainframe vulnerability management lifecycle in half the time of those in the Not Ready and Complacent groups.** In an examination of the amount of time it takes to complete critical vulnerability management tasks — from scanning for vulnerabilities all the way to reporting on the results of patching — we found that it takes the Not Ready group (41.7 business days) and Complacent group (44.6 business days) twice as long to complete the mainframe vulnerability lifecycle than the Ready group (20.0 business days) (see Figure 9)! Having a more advanced, mature approach to mainframe security greatly reduces the time to resolve critical vulnerabilities that could have a major impact on organizations.

Mature organizations can complete the mainframe vulnerability management lifecycle in half the time of those in the Not Ready and Complacent groups.

Figure 9: More Mature Companies Save Time On Vulnerability Management

"To the best of your knowledge, how long does it take you on average to do the following tasks in the mainframe vulnerability management lifecycle?"

	Not Ready	Complacent	Ready
Scan your mainframe for critical vulnerabilities or misconfigurations	7.9	8.6	3.1
Coordinate scan results between your teams	5.6	6.3	3.0
Patch critical vulnerabilities	7.1	7.3	3.6
Deploy updates	6.9	6.9	3.6
Rescan your mainframe to ensure patch or deployment has been applied	6.4	7.4	3.2
Report on the results of your patching and deployment efforts	7.8	8.1	3.5
Total Business Days:	**41.7**	**44.6**	**20.0**

Base: 264 security decision makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

- **A reliable, secure mainframe moves beyond operational benefits alone to bolster reliability and customer trust.** Brand protection and the trust of customers is critical to winning and retaining a customer base. When there is any sort of data breach, customers are often quick to move on to another company. The manager of mainframe computer operations at a transportation/logistics company noted just how critical the security of the mainframe is to their overall customer objectives:

> *"The biggest part of having a reliable network on the mainframe side is getting the trust of your customer. Period. If you have improved security, you can expect your customers to keep coming because they know your network is absolutely secure. All the customers have to do is their business, and not worry about anything else like people compromising their data."*

"If you have improved security, you can expect your customers to keep coming."

- **With improved security, companies would move more workloads to the mainframe.** Respondents agreed that if their organizations could secure the mainframe, they would move even more workloads there as a result of the reliability is provides. As one CISO and VP at a financial technology company noted:

> *"If we decided that the mainframe was a more strategic and secure platform, we would use it in use cases that we don't today."*

Key Recommendations

According to recent Forrester research, 58% of infrastructure technology decision makers today use mainframes. In fact, 46% of respondents said their organizations plan to increase their use of mainframe over the next two years, and another 39% predict it will stay the same.[2] It's not too late to improve mainframe security and elevate it to the level of other security disciplines. Forrester's in-depth survey of mainframe security decision makers yielded several important recommendations:

Get a baseline of what your mainframe security posture is. To improve, you first need to know where you are. Use a penetration test to prioritize your security gaps. Also, review what tools and technologies you can use for both the mainframe and other security disciplines. Are you using the same tools for mainframe whenever possible? This will help you create and respond to consistent security policies.

Change your definition of "regularly" when it comes to security tasks. You can gain speed on mainframe vulnerability management, but you must first increase your pace of performing critical mainframe security tasks such as penetration testing, vulnerability scanning, and configuration management. Take a note from more mature organizations on how often you should perform these tasks. For example, only 17% of the Not Ready group and 21% of the Complacent group consider "regular" penetration testing to be monthly, while more than double that amount (44%) of the Ready group said regular testing should take place on a monthly basis. It's the same for vulnerability scanning: The Not Ready group (27%) and Complacent group (25%) consider regular testing to be monthly, which is far less frequent than the Ready group (57%) tests. Target to perform these tasks monthly, but fall back to quarterly if you experience budget or personnel restrictions.

Fill your mainframe security talent gap creatively. Cross-training of existing security professionals to perform mainframe security is always an option. However, if you lack expertise for mainframe security, managed service providers can help fill in the gaps. Finally, if hiring for mainframe security is an option, you will be hard-pressed to find individuals with significant experience.[3] Instead, seek out those with intellect, motivation, and fit, and tap into nontraditional sources such as veterans and women (who have historically not been hired for these roles).[4] You need to target individuals who enjoy conquering difficult problems and are genuinely interested because they understand the career opportunity it represents: becoming a sought-after security expert in a mission-critical technology.

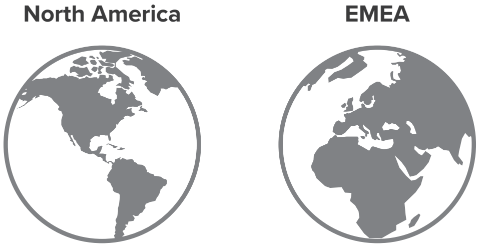
Include mainframe in your security information and event management (SIEM). You don't have to wait for an internal audit to understand what is happening on your mainframe. Leverage the SIEM you have to automatically include mainframe log data to get up-to-date information on what is going on and highlight any security events you need to triage and eventually investigate based on severity and criticality.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 264 security decision makers and interviewed four security decision makers in North America and EMEA with insights into mainframe security at enterprises across all industries to evaluate mainframe security practices and perceptions. Study participants included manager-level and above decision makers. The study was completed in May 2020.

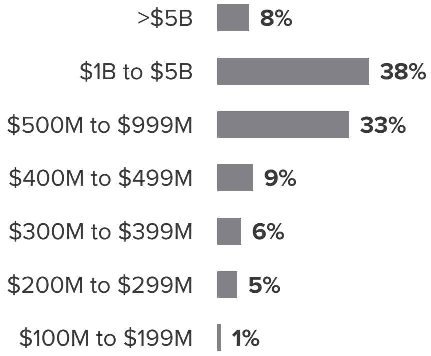
Appendix B: Demographics/Data

GEOGRAPHY

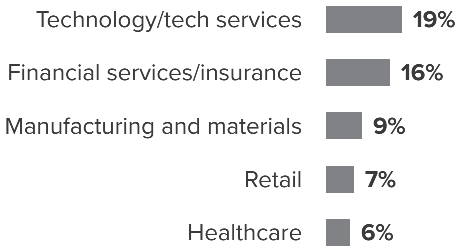


North America		EMEA	
US	**43%**	UK	**16%**
Canada	**11%**	Spain	**8%**
		Italy	**8%**
		France	**8%**
		Germany	**6%**

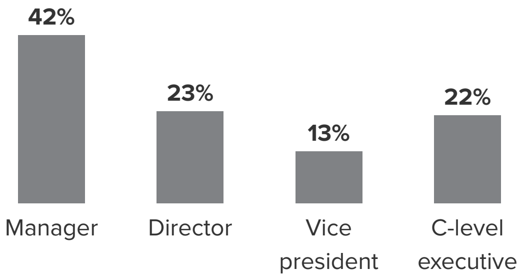
COMPANY SIZE
(BY ANNUAL REVENUE IN USD)



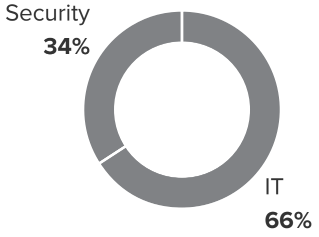
INDUSTRY
(CROSS-INDUSTRY, TOP 6 SHOWN)



RESPONDENT LEVEL



DEPARTMENT



100% are decision makers for mainframe security.

Base: 264 security decision makers in North America and EMEA with insights into mainframe security
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, May 2020

Appendix C: Endnotes And Supplemental Research

[1] Mainframe Security Readiness Model calculation: This research explored the readiness of organizations to prepare and secure the mainframe for the modern IT enterprise. It analyzed 14 factors of mainframe readiness including the perception of mainframe security, the organization's attitude toward mainframe security, mainframe security risks experienced by the organization, and the level of screening/visibility/security features in place. The scales for each question were ranked by least ready (1) to most ready (5). The sum of these values indicates the mainframe readiness score of each respondent. Respondents were grouped into three tiers based on their aggregate scores: Not Ready, Complacent, and Ready. Not Ready represents an average score of 1.0 to 3.4; Complacent represents an average score of 3.5 to 4.0; and Ready represents an average score of 4.1 to 5.0.

[2] Source: Source: Forrester Analytics Business Technographics® Global Infrastructure Survey, 2019, Forrester Research, Inc.

[3] Source: "Tackling The Unsexy Challenge Of Mainframe Modernization," Forrester Research, Inc., December 21, 2018.

[4] Source: "Reverse Cybersecurity's Self-Inflicted Staffing Shortage," Forrester Research, Inc., July 18, 2019.