Mitigating Mainframe Security Risks with Endpoint Detection and Response

8 Steps Manufacturers Should Take to Shore up Your Defense Against Cyberattack
Table of Contents

01  Introduction
02  Houston, We Have a People Problem!
03  Coping with the Cost of a Breach 8 Steps
04  Conclusion
Introduction

Big iron. Sounds indestructible, right? Reliability is indeed an advantage of mainframes, and it’s one of the primary reasons they have anchored the IT systems of Global 500 enterprises for more than 50 years. In fact, despite claims that mainframes are going the same route as the dinosaurs, they’re still in use by 70% of Global 500 companies¹ with a mean time between failures (MTBF) that’s commonly measured in years.² The problem is that these systems, relied upon to meet vital bulk data and transaction processing needs, are facing a greater cybersecurity risk than we truly realize.

The cybersecurity landscape is more like an ocean, with currents and patterns that constantly shift in response to trends around the world. Today, cybercrime isn’t some cottage industry with a few bad actors – it’s an enterprise in itself, with well-funded nation-state attackers training armies of cyber soldiers.³ Criminal organizations are also selling Malware as a Service, allowing would-be cybercriminals with little-to-no working knowledge of programming to pose a significant threat to enterprises that don’t have the proper security measures in place. The GandCrab ransomware exploit that emerged in 2017 is a prime example, and developers shared the kit on a forum with the condition that they would keep 60% of ransom fees for themselves.⁴ The criminals even went so far as to offer customer service that included user (hacker) support and updates. As the cybercrime industry matures, it’s no wonder CISOs are feeling the pressure.

A study from the University of Maryland’s Clark School of Engineering indicates that computers with internet access are subject to an average of 2,244 attempted intrusions every day,⁵ and research from the Ponemon Institute illustrates that 67% of CISOs felt they were more likely to suffer a cyberattack in 2018 versus 2017. Of those digital leaders, 56% blamed the increasing sophistication and stealth of their attackers.⁶ Unfortunately, attacks aren’t a CISO’s only concern.

A significant portion of security measures aren’t about preventing cyberattacks – they’re about ensuring compliance with whatever security standards govern your particular industry. In addition to the alphabet soup that includes PCI DSS, HIPAA, FISMA, ISO 27001, GLBA, FFIEC, IRS Pub. 1075, and a host of others, governments are passing their own standards. The European Union’s General Data Protection Regulation (GDPR), which became enforceable on May 25, 2018 after being adopted more than two years earlier, was one of the first modern regulations designed to protect citizens’ data and privacy.

¹ https://www.itpro.co.uk/server/29990/why-the-mainframe-is-still-going-strong
³ https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/
⁵ https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
GDPR carries severe consequences for both companies and individuals responsible for data mismanagement, and it governs all data handling organizations with “data subjects” residing within European borders. In addition to doling out punishments to organizations that lose or misuse data, it lays out a framework of steps that organizations (including non-profits) must take to demonstrate their commitment to protecting EU citizens’ personal data.

The GDPR has had far-reaching effects, including the inspiration of similar data protection regulations in the United States. California passed the California Consumer Privacy Act (CCPA) in 2018, and eleven states quickly put forth their own legislation regarding data protection. Now, that number has grown to 25, and bodies such as the U.S. Chamber of Commerce are calling for a federal privacy law to protect consumer data. Following President Trump’s 2018 creation of the Cybersecurity and Infrastructure Security Agency (CISA), experts such as former FTC commissioner and current Microsoft vice president of privacy Julie Brill, think the U.S. government will pass its own sweeping regulation, applying further pressure on CIOs.

---

Houston, We Have a People Problem!

IT departments have more on their plates than ever before, but the persistent view of IT as a cost center continues to prevent departments from getting access to the skilled workers they need to deliver IT services on time and to acceptable SLAs. According to a survey from Spiceworks, the average IT professional puts in 52 hours of work per week, and 18% of respondents exceed 60 hours each week. Indeed, human resource management, including training existing employees and hiring additional staff, is the second highest priority for CIOs in 2019 behind security.

With resources stretched thin, IT departments don’t have the bodies to adequately protect the distributed systems running corporate Security Information & Event Management (SIEM) software and appliances. And these traditional defenses on distributed systems aren’t interoperable enough to protect valuable mainframe data and IP. Anti-virus systems can be a viable defense against well-established threats on distributed systems, but these measures are often useless against the cutting-edge, 0-day malware that is constantly under development on the front lines of cyber warfare. IT Firewalls have also become little more than a speedbump for today’s hackers because your network access spans wider and farther out than ever. Whereas a mere 20 years ago network access mostly covered servers with connectivity, the advent of the mobile device has created an exponential and unmanageable rise in the number of network access points with each a potential intrusion vehicle.

Now, the mainframe has become a TCP/IP-connected computer that’s integrated with your enterprise, meaning it must be treated like any other endpoint. With 360,000-plus malicious viruses introduced to the world’s computers on a daily basis, manual cybersecurity solutions can’t possibly keep up. At a rate this volatile, even hourly virus definition updates are not enough. Instead, enterprises must put automated solutions in place that support their agile organizations with real-time correlation reports and endpoint security monitoring.

What is your current strategy costing you? According to independent research conducted by the Ponemon Institute, the mean time for an organization to identify and contain a data breach in 2019 was a staggering 279 days. Six-plus months is a long time for bad actors to have covert access to enterprise data and IP, but many have gone longer including a breach at Marriott that went unnoticed for almost four years. The numbers today tell a sobering story about cybercrime for those of us hoping to minimize the collateral damage from a breach – we don’t even know when they are happening.

11 http://www.itmanagerdaily.com/survey-it-pros-are-seriously-overworked/
Coping with the Cost of a Breach

So, your network has been breached. If only it were as simple as plugging a hole. Once a cybercriminal has penetrated the outer perimeter of your firewall, they have access to just about everything inside it. A privileged user could theoretically access every username and password stored in your system, escalate administrative permissions for whomever they are working with, and create new backdoor access points in order to maintain control once you think you’ve completed remediation. Cleaning up this mess isn’t going to be cheap – and that is if you even notice it at all.

In addition to the substantial price tag associated with mitigation and restoration efforts, you’re also on the hook for hefty fines, potential ransom payments to attackers, the cost of litigation, and the intangible loss in customer trust that accompanies a breach. With so many factors contributing to the rising price of a security incident, it’s no surprise the average data breach costs $3.92 million, according to Ponemon’s “2019 Cost of a Data Breach” global study.14 That number will continue to grow in the years to come, threatening both companies and the careers of CxOs who hold watch over Personally Identifiable Information (PII) and corporate IP. In some cases, costs can be much higher, such as the $148 million penalty levied against Uber for its 2016 violation of state data breach notification laws.16

When a breach of Anthem affected 79 million customers in 2015, the $16 million fine for HIPAA violations17 was drastically overshadowed by the $115 million settlement the insurer reached in a class action lawsuit.18

Because mainframes are an incredibly valuable source of data, they are always under threat.

While there’s no definitive action you can take to avoid becoming the next victim in data breach headlines, the following steps will go a long way toward insulating your organization from the risk.

1. **Security Operations Center (SOC) Inclusion:**
   All too often, security is compromised because it’s separated into two different worlds: the mainframe world and the distributed world. Instead, the SOC should grant security personnel a 360-degree view of all data, including SIEM data generated by the mainframe. Breaches aren’t platform-specific, and neither is your enterprise. With the SOC keeping a watchful eye on both distributed and mainframe events, suspicious activity can be spotted and reported before a problem gets worse.

2. **Rely on Real-time Mainframe Reporting:**
   Most mainframe reporting happens on a nightly or weekly basis. That level of monitoring is no longer acceptable when every second counts towards containing data exfiltration. Today’s SIEM must include real-time mainframe security events – alongside WIN/UNIX/open source – that automatically alert security admins and support staff if any anomalous behavior is detected. Considering mainframes power stock exchanges, ATMs, and major e-commerce platforms, a few minutes of downtime can cost your organization a fortune.

---

18 [https://www.gdpreu.org/compliance/finances-and-penalties/](https://www.gdpreu.org/compliance/finances-and-penalties/)
3. **Count on Correlation:** Correlation is a powerful tool to deepen your understanding of what’s going on in your organization’s environment, and BMC’s correlation engine is best-in-class. With our automated event management system powered by expert designed Indicators of Compromise (IOC), you’re quickly notified of suspicious and potentially malicious activity outside the normal scope of day-to-day operations. Because of the automation built into the system, your organization can take quick, decisive action to minimize the risk associated with breaches without having to rely on your already-stretched-thin IT team.

4. **Monitor Privileged Users:** The mainframe is your most valuable IT asset, and privileged users have unrestricted access. When Gottfrid Svartholm hacked into the mainframe of Swedish IT firm Logica and stole tens of thousands of user accounts, one of his first moves was to escalate the privileges of users so he could maintain access when admins noticed the hack and changed their passwords. In addition to ever-present external threats, a survey of more than 500 IT decision-makers in Europe found that only 9% felt insulated from insider threats, and 42% of respondents in the UK felt that privileged users were the biggest source of risk to their companies. With BMC’s Automated Mainframe Intelligence (AMI) for Security, you can actively monitor privileged users and set up alerts based on correlation rules to identify anomalous activity.

5. **Vet your Vendors:** Most security tools run on UNIX and open source systems and are managed by resources who have never touched a mainframe. Because the people and systems managing enterprise security aren’t mainframers, you are most likely at high risk to protect the wealth of valuable data housed on your organization’s mainframe. For nearly 40 years, BMC’s focus has been mainframe technologies, and BMC’s AMI for Security was designed specifically with mainframe security in mind. With an IT asset as critical to daily business as the mainframe, settling for a non-specific security solution is like opting to protect your home with car insurance.

6. **Test Response Readiness:** A study conducted by the Ponemon Institute in partnership with IBM recently found that 77% of organizations lacked a cybersecurity incident response plan. Still, having a plan doesn’t necessarily mean you’re prepared. In the same way schools and workplaces hold regular fire drills, you should test your response to a breach on a regular basis to ensure your employees know their roles and can perform them under pressure. Need an incentive? Responding to an attack within 30 days will save you an average of $1 million per incident.

7. **Lean on Your Legal Team:** Many organizations only look to the legal team to clean up the mess of a data breach, but they can also be a great resource before an incident happens. Your legal team should have good experience with cybersecurity compliance regulations such as the GDPR and current U.S. states’ legislation, and they will also have information on the latest state PII laws coming into effect in the U.S. They will also be familiar with what’s covered in your cybersecurity insurance policy in the event you ever need it.

---

This experience means they can help educate your entire organization about the risks associated with managing PII, the key protected component in the latest data security laws in the U.S. Ignorance of the rules is no excuse, and data protection regulations present stiff penalties. For companies with customers living in the European Union, GDPR infringements can carry a penalty of €20 million or 4% of the prior year’s revenue – whichever is greater. Clearly, you’re better off on the right side of the law.

8. Continuing Employee Cyber-Education:
Human error continues to haunt companies, and research by London consulting firm Willis Towers Watson indicates that about 90% of all cyber insurance claims stem from employee malice or negligence. Shore up your cyber defenses by educating employees about cybersecurity best practices, particularly since non-technical departments such as marketing are now taking control of PII to create customer interactions that IT security operations may never be aware of. With these new PII laws in the U.S., “John Q. Public” now controls how you manage your data and your entire team needs to understand the risk.

In the past, it was easy to take mainframe security for granted. The mainframe was locked down behind closed doors, and even if you were able to get into the room, you’d still needed the coding experience to hack it. Today, the mainframe is closer to the internet than ever before, and it’s powering the bulk of the world’s credit card purchases with speed and volume measured in millions of transactions per second. Now, with CICS on z/OS managing these transactions, both hackers and cybersecurity researchers are illustrating how “the most secure platform on Earth” is more susceptible than anyone thought. While even the most well-intentioned cybersecurity defenses can fall victim to human error or negligence, you can and should take responsible steps to insulate your organization from risk.

22 https://www.gdpreu.org/compliance/fines-and-penalties/
23 https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/
Conclusion

In the past, it was easy to take mainframe security for granted. The mainframe was locked down behind closed doors, and even if you were able to get into the room, you’d still needed the coding experience to hack it. Today, the mainframe is closer to the internet than ever before, and it’s powering the bulk of the world’s credit card purchases with speed and volume measured in millions of transactions per second.

Now, with CICS on z/OS managing these transactions, both hackers and cybersecurity researchers are illustrating how “the most secure platform on Earth” is more susceptible than anyone thought. While even the most well-intentioned cybersecurity defenses can fall victim to human error or negligence, you can and should take responsible steps to insulate your organization from risk.


For more information
To learn more about AMI for Security, BMC’s latest mainframe security product family, please visit our product page, or reach out to a BMC expert today.