CROSSING THE CISO – MAINFRAME CHASM

A comedian once lamented “Let me tell ya, I don’t get no respect”. Welcome to the life of the chief information security officer (CISO), where large organizations get attacked millions of times each day and the CISO and security teams need to be right virtually 100% of the time. It’s not surprising that the primary concern that keeps a CISO “up at night” is an attacker that successfully penetrates the mesh defense systems designed to prevent intrusion and attacks.

But seasoned CISOs know that there is another concern that haunts them even after the last emails of the day have been addressed: What do I not know that could harm me?

The latest hot new CISO focus

As IT professionals, we are expected to have reasonably high competence across multiple platforms and infrastructure. CISOs are tasked with governance models, implementation of complex policies, validation of adherence to policies, establishing monitoring procedures to alert organizations to potential threats, creating response programs to address the unlikely event of a successful attack **and** reporting to the board on progress or gaps in the security posture of the organization.

With the advent of cloud and organizational adoption of this “pay as you use” computing resource, protecting those corporate IT assets is a critical new challenge that is taking top priority for CISOs across the world. It’s big, it’s new and it has already proven to be a vulnerable attack surface for threat actors (see the Capital One attack, for example). It requires learning quickly how the organization is leveraging cloud computing, understanding/addressing security risks and proactively identifying new vulnerabilities that could be introduced. Advances in artificial intelligence (AI) only add to the large threat landscape that CISOs must defend against.

Enter the awkward CISO discussion about mainframes

Distributed systems and cloud infrastructure have dominated the IT conversation for the past 30 years. Consequently, most CISOs have very little knowledge of mainframes, and it's not something that they necessarily want to illuminate. "Not knowing" or "not knowing enough" is not a good look for an executive. For organizations with mainframe computers, there is also an ominous truth that all CISOs quickly acknowledge – if the mainframe stops, the business stops. An extended mainframe outage is an existential threat to the high-profile organizations that comprise the financial backbone of our society.

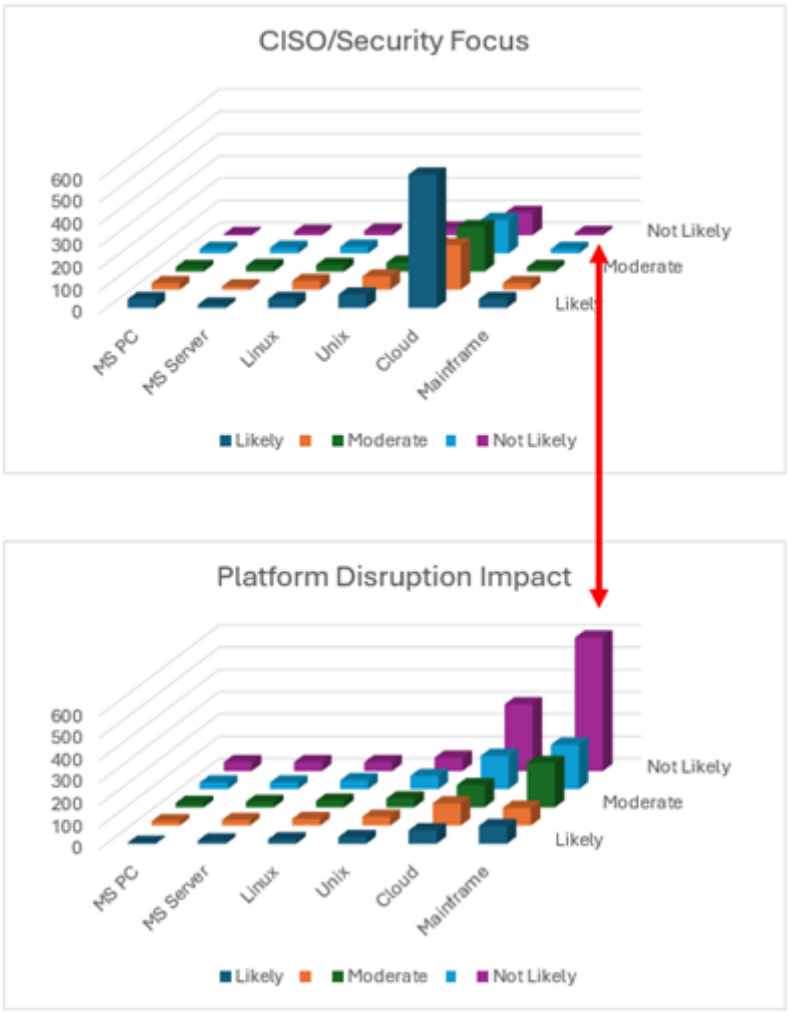

Figure 1: Crossing the CISO – Mainframe Chasm

Key differences between mainframe and distributed systems security

There are a few key security differences between the mainframe and distributed systems platforms. While mainframe perimeters tend to be well-controlled, nearly all successful mainframe attacks occur from internal actors gone rogue or threat actors that have obtained valid credentials. There are a number of ways to gain complete control of a mainframe above and beyond privilege escalation and full control is a dangerous state for a user on your mainframe. Additionally, many CISOs are unaware that the mainframe hosts thousands to tens (sometimes hundreds) of thousands of users, many of whom are contractors – a source of many mainframe attacks. The internet has many sites that educate and facilitate attack points for the mainframe – easily accessed and

digestible to enhance mainframe skills that can be used to prepare for an attack. Finally, the mainframe lacks scanning tools to detect malware, ransomware, and malicious encryption - tools that are readily available on distributed systems platforms. Consequently, real-time monitoring becomes critical to detect malicious activity on the mainframe.

CISO action plan for mainframe platforms

Interestingly, the mainframe security action plan for CISOs is similar to key compliance regulations (Digital Operational Resilience Act (DORA), Network and Information Systems Directive 2 (NIS2), etc.).

- Confirm that the mainframe is critical infrastructure (for most organizations with mainframes, the answer is yes).
- Assess the security posture of your mainframe by performing a penetration test (pentest) examining the internal configurations, user access and vulnerabilities. Hint: "Not knowing" is itself a vulnerability that many CISOs have come to acknowledge.
- Understand security monitoring on your mainframe.
    - Your login system (RACF, Top Secret or ACF2) is not sufficient to detect threats – just as Windows security isn't sufficient protection for your Windows servers.
    - Does your mainframe security monitoring detect and send meaningful security alerts to your security information and event management (SIEM) in real time to provide an enterprise view of security threats?
- Develop a remediation plan to improve your mainframe security posture.
    - Many mainframes have hundreds or thousands of user IDs that have not been accessed in over 2 years. These are vulnerability points.
    - Many users are over-provisioned for privileges or access.

Crossing the CISO – mainframe chasm: Summary

CISO governance models and procedures are critical for corporate security, but mainframes are often overlooked as legacy platforms that are assumed to be secure. This leads to CISOs "not knowing" the security posture or vulnerabilities of the mainframe platform.

For organizations that leverage the power of mainframes, those mainframes are critical infrastructure that the entire business depends on – if the mainframe stops, business stops.

Key steps for CISOs to incorporate their mainframes into their governance, risk and security strategy:

- Confirm that your mainframe is critical to organizational processes.
- Penetration test the mainframe infrastructure - not just the perimeter.
- Ensure real-time mainframe security monitoring is incorporated into your corporate SIEM.
- Develop remediation plans to address pentest vulnerabilities.

To learn more about how BMC can help your organization strengthen its mainframe security, visit the BMC AMI Security webpage.