How to Deliver a Mainframe Security Hardening Program

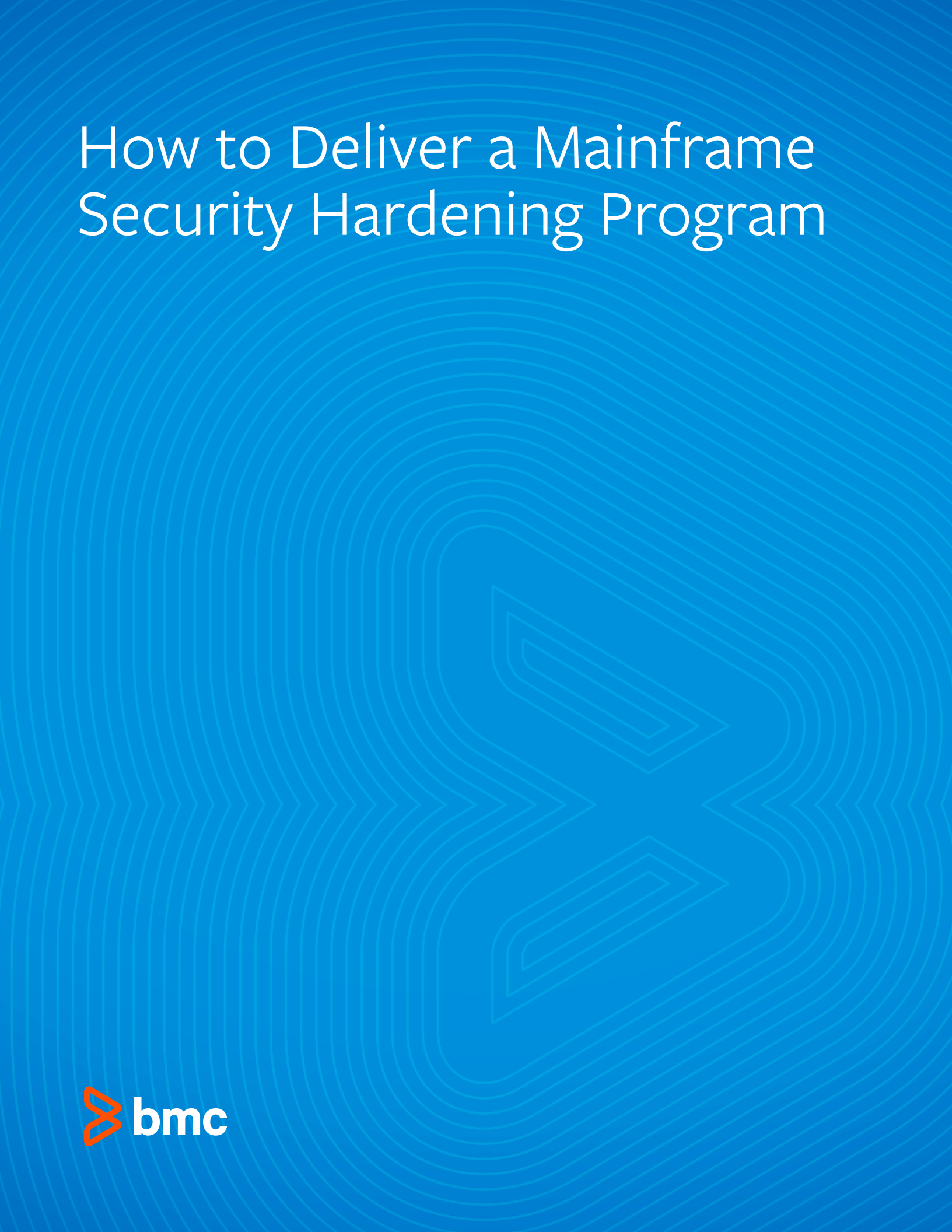

Table of Contents

Introduction

People, Process and Technology:
Seven Steps to a More Secure Enterprise

The mainframe is the processing and transactional heart of many organizations: part of our critical national infrastructure. Yet even in an era that is characterized by data breaches, evolving cyber threats and heightened awareness, the mainframe has been the poor cousin of the enterprise: often underfunded and so often resulting in a high number of vulnerabilities that place the central processing hub at risk from internal and external threats. Despite tougher regulatory regimes, the threat of huge fines and reputational damage, some mainframe sites are still failing to comply.

However, the people, processes and technology required to deliver a robust mainframe security stance are already available. Perhaps a change in mainframe culture and mindset is one of the missing pieces of the jigsaw?

The opportunity is to build stronger and more sustainable controls that protect the crown jewels of the enterprise whilst simultaneously meeting the demands and expectations of stakeholders that include analysts, auditors, boards of directors, regulators, customers and the media.

The Scale of the Problem

Too many organizations are not considering what would happen if an internal or external threat sabotaged or otherwise disabled their systems. In every location that we conduct a security audit or pen test, we always find significant security concerns that expose highly sensitive data. From a file containing credit card details for all customers to powerful userids with default passwords, there is always something for hackers to exploit.

Indeed, we continue to see a trend of sites with extremely weak controls, a trend that is also consistently revealed in industry surveys. For example, in the July 2020 Forrester report *A False Sense of Mainframe Security*, more than 80% of IT leaders surveyed said that even though they have the right tools in place, they still experience major security events. Of even greater concern is that while data protection and risk reduction are considered top IT priorities, three-fifths of organizations are not taking the steps required to actually secure their mainframes. 42% of respondents reported that someone had gained unauthenticated access to their mainframe. 39% said user privileges had been elevated without their knowledge.

Of course, some sites are better than others, notably those in financial services, but many of those still have significant room for improvement. What is the root cause? Part of the problem is that the platform has been around for a long time. If you ask managers why they haven't invested in better controls, many will say "Because we don't need to: the mainframe is secure." According to BMC Software's John McKenny, mainframe security overconfidence "is essentially due to the fact organizations are often mistaken to believe that 'secure' is inherent for mainframes. In reality, secure means 'securable'."

[1] *A False Sense of Mainframe Security* – a commissioned study by Forrester Consulting on behalf of BMC Software, July 2020

The Mainframe is Not Inherently Secure

It is important to reinforce just how dependent we are on the mainframe, on the data it holds and the services it provides, and across sectors including banking, retail, travel and utilities. The platform is part of our critical national infrastructure. Yet how many times have we heard some people say, "We are not really investing in the mainframe ... it's legacy ... we will be moving to other platforms." In so many cases, while that never happened, the required investments in appropriate controls were never made. So the question to pose to managers is, "If you were to switch off that machine today, or if it was sabotaged, what would be the impact on your business and your customers?"

For some, it could mean that 90% of their business would effectively fail. Transactions would cease as processing stops, with all the dependencies on that. Parts of the organization and its operations would be paralyzed. But many have lost sight of this dependency. The good news is that we are starting to see more awareness and improvements in controls, but there is still a long way to go.

The mainframe is probably the most *securable* platform on the planet but is not inherently secure. As a result, people may have a false sense of security. Budgetary constraints and requirements considered to be "more pressing" such as newer technologies or reassigned priorities compound the issue. The reality is that the mainframe is as prone to hacking as any other platform. We constantly see examples of poorly configured access controls, exposure of sensitive operating system resources, and excessive levels of access because so many organizations have resolutely failed to clean up unused access. It is time for action.

"Pen testing's main objective is to identify security weaknesses, which can then be remediated, thus improving an organization's security posture. It can also be used to test an organization's security policies, its adherence to compliance requirements, its employees' security awareness, and the ability of the enterprise to identify and respond to security incidents."
— *Mark Wilson, BMC Mainframe Services by RSM Partners*

Taking Action: Ten Steps

This is a journey of continuous improvement rather than a one-time exercise.

It is important early on to identify the extent of the problem. This often means using external specialists to conduct penetration tests followed by a full security assessment, to properly understand the scope of the challenges and inform all remedial action required. The value of this approach extends far beyond the proof delivered by a pen test that your current security posture is simply not enough. The ten steps are:

Step 1.
Recognizing the issues and being honest about your security challenges.

Step 2.
Pen Testing via an expert external source.

Step 3.
Performing a detailed audit through a *Security Assessment*.

Step 4.
Prioritizing action using a *Risk Assessment*.

Step 5.
Developing and documenting your *Remediation Plan* based on those priorities.

Step 6.
Gaining top-down *management support* for your security hardening program.

Step 7.
Ongoing *reviews and testing* of controls to verify their effectiveness.

Step 8.
Research and exploit the latest innovations in your security software.

Step 9.
Invest in education and training for your Mainframe Security professionals to keep their skills and knowledge current.

Step 10.
Implement a Mainframe *Security Engineering* practice to help build and maintain a strong security posture.

By deploying people, process and technology in the most appropriate ways, a properly planned and executed mainframe security hardening program results in a central processing hub that provides strong and effective security and integrity of customer data and intellectual property, reducing operational risk. Protecting that data and IP is paramount. Such an approach also helps an organization to maintain its reputation in the marketplace as it is less likely to suffer badly from a security incident or breach. All stakeholders, internal and external, can have greater confidence in your ability to reduce and manage risks to the business, while customer confidence is also enhanced.

Pen Tests: ‘Cards on the Table’

When organizations use their internal audit function for a security assessment or perhaps one of big consultancy firms, the individuals are generally not armed with the knowledge and skills to take a proper look “under the hood”. This can result in a tick-box audit, superficial in nature. By contrast, pen testing by objective experts is a valuable way to focus minds, surfacing real-life security problems, risks to be addressed and gaps to be closed.

This “cards on the table” approach is one of the best ways to enact much-needed change and secure extra budget for security. For the organization, it does mean giving trusted external experts access to all systems so they can go as deep as necessary. The findings can trigger a genuine focus on real-world problems.

Pen tests can also provide a useful way to get an organization’s internal audit function onside, by explaining to them the extent of the security issues and helping them to develop their understanding of both the threats and the mechanics of putting it right. Working in an open and transparent can open minds and change attitudes.

Working together, mainframe and internal audit teams can then present a strong case for the board to provide budget for more detailed investigations and necessary remediation work. The often-seen alternative, however, is for managers to say, “Great, get it on the risk register as there’s no money to solve it.” Again, this is why a detailed approach by an independent third party using industry best practice and ideally liaising with the internal audit function can be a powerful catalyst to implement the necessary controls.

Taking Control: People – Process – Technology

Once the scale of the problem is understood, the next step is prioritizing the most important areas to fix, and so remove the highest areas of risk. This is typically driven by a Risk Assessment that feeds into a documented Remediation Plan: what to fix, where, in what order, and how to fix it. This planning is critical. Again, using an independent provider for the Risk Assessment is important to ensure an objective eye in deciding on the priorities for a specific set-up and the organization's particular business or operating requirements. In an ideal world, the client organization maps this assessment, the various risks and priorities, to their own risk models and methodologies.

Having a strong plan, while vitally important, is only an interim stage between "properly understanding your security problems" and "arriving at a far stronger, more resilient and adaptable security and governance posture". Any security improvement program will falter without the support of senior managers in terms of buy-in, focus and budget. The plan, and the people implementing it, need that top-down management support to succeed.

Inadequate security and weak controls are often a result of:

- Not having the right people on the ground: insufficient headcount, poor resourcing.
- Mainframe and security processes that are no longer fit-for-purpose or simply do not exist.
- Outdated (or simply no) technologies and tools to support mainframe security: perhaps 25-year-old homegrown software, or using only a fraction of the capabilities of current tools.

All three areas need to be addressed, and all are fixable. For example:

- **People:** if you face headcount issues, look outside the organization for independent expertise, in particular to enable knowledge transfer to upskill your in-house mainframe and audit teams.
- **Technology:** solutions are available that can help. This can include purchasing fit-for-purpose software and tools from trusted providers such as IBM, BMC and ISVs, but always making sure they align with your specific security needs and/or ensuring they mitigate the risks that have been prioritized in your plan.
- **Process:** arrange a Pen Test followed by a Security Assessment, including Risk Assessment and Remediation Plan, all executed with management support.

Maintain Momentum: Continuous Improvement

Once these areas have been addressed, or are in progress, it's important to continue on your security journey and to ensure all your good work to date does not fall by the wayside. We have seen on numerous occasions that organizations carry out a security audit and identify problems to fix, from access reduction onwards, and start to get their house in order – then everything stops when another project or new priority emerges. But access reduction, like so many other mainframe and security activities, should never cease.

It does not matter how much groundwork you do, or practical steps you take to seal the gaps, the moment you turn your back, controls start to unravel very quickly – and you are back in a similar place to where you started. This can happen fast, in weeks or days. The reality is that the smallest issues can result in a huge exposure on the system, something an organization may not be aware of until a serious data breach hits.

Getting it Right: Reduce Your Exposure

The Prize? Gaining a More Secure, Robust and Resilient Mainframe Environment

At a basic level, pursuing a security improvement and hardening approach should, in itself, help to effect a change in mindset for the people within the organization entrusted with securing the mainframe. This new mindset should also mean this is a not a one-off: it becomes how you do things.

The enterprise in general will benefit from a significant risk reduction in terms of unauthorized access, data breaches and internal threats. This can not only help to increase confidence within and outside the organization – while avoiding significant financial penalties and longstanding reputational damage - but also means you can demonstrate that capability to investors and industry regulators. This means you are less likely to be placed under the microscope for scrutiny: you have it under control. Longer-term, you can aim to reduce costs and save money through the increased efficiency and productivity of your mainframe platform.

In fact, we believe there is a significant and continued return on investment, all be it very difficult to quantify. How can you quantify "the road not taken" when it comes to security breaches and data losses that never actually happened thanks to your improved security posture?

10 outcomes of a successful security hardening program:

1. Providing a robust and up to date security stance for the enterprise.
2. Delivering a significant reduction in risk for critical assets via improved protections.
3. Greatly reduced risk of breaches, reputational damage, and large fines.
4. A reduction in audit findings, with less time spent on remediation.
5. Gaining complete visibility of controls and enabling swift action to fix non-compliant controls.
6. Reducing the scope for security breaches from both insider and external threats.
7. Compliance with internal security policies and standards.
8. Compliance with external regulatory and legal requirements.
9. Improved platform productivity.
10. Enabling positive messages for all stakeholders on your security and data confidentiality regime: employees, customers, partners, investors, and the media.

Need help Securing your Mainframe?
Connect with an Expert here.

About BMC
From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent **www.bmc.com**

bmc

BMC, the BMC logo, and BMC's other product names are the exclusive properties of BMC Software, Inc. or its affiliates, are registered or pending registration with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other trademarks or registered trademarks are the property of their respective owners.
© Copyright 2020 BMC Software, Inc.

524835