MST Resilience Case Study 2022

Reputation is everything!

> We know that organisations will fall victim to cyber-attacks, it's happening daily, and the attackers seem to be getting more sophisticated. Cyber-attacks can take many forms, from phishing and malware to exploiting vulnerabilities and ransomware. The threats and modus operandi are different, but they all have one thing in common - they all represent a significant business risk to your business, and you need to take precautions.

David Cohen
Moore Cyber Johannesburg Managing Director

Professional service firms have access to vast and varied client information. Their clients trust them implicitly with their private and confidential information. Any breach of information could prove catastrophic to a professional services firm reputation.

Reputation is everything!

With this in mind, the MST decided to commit to a process of building up their cyber resilience and improving their cyber posture. The real issue facing the directors was where to start.

Cyber is spoken about at board meetings and strategic sessions, but for most, the horrific stories about Cyber hacks remain either entertaining or intriguing with little or no change in company focus or strategy.

This was not the case for MST, who sat down and consulted with Cyber specialists about defining a cyber plan to align the organisation's risk appetite with best practice and to ensure they followed a verifiable, tried and tested methodology in their journey toward "cyber readiness."

Knowing that no company will be "cyber safe", MST chose to follow a cyber resilience roadmap that would give them the best cyber protection in the shortest amount of time.

They were also insistent on receiving a full cyber remediation roadmap and project plan as an essential output of their stated objectives.

OBJECTIVE

Understand the cyber risk landscape and how it impacts MST's business

Gain valuable insight into their IT and infosec environment both externally and internally through a vulnerability assessment and penetration test

Train their staff in cyber awareness to reduce the effects of social engineering, which is used in up to 90% of all cyber attacks

Have a detailed remediation roadmap and project plan to address all identified risks logically and practically

UNDERSTANDING THE CYBER RESILIENCE ROADMAP AND REMEDIATION STRATEGY WAS A CRITICAL FIRST STEP FOR MST

Drivers	**Business** • Strategies • Treats • Risk Tolerance	**IT** • Strategies • Architecture • Organization	**Compilation** • Methodology • Data • Standards
Enterprise Security Framework	**Security operations** • Access Management • Directory Management • Authentication • User Administration • Remote Access • Application Security • Pen Test/ Ethical Hack • Change Management • Vulnerability Management • Patch Management • End point Security • Data protection & Encryption	**Governance** • Security program policies • Standards and Procedures • Threat & Risk Assessment • Risk Management • Metrics & Reporting Asset • Classification Awareness • Security Assessments • Remediation Management • Vulnerability alerting • Vendor Management	**Independent Response** • Incident Detection • Incident response plan • Disaster recovery plan • Data restoration System monitoring • Log control • Event management • Escalation • Enterprise response plan • Communication plan
Processes	**People / Organization** • Roles & Responsibility • Training • Awareness	**Risk Management** • Third Party Vendor Risk • Risk Transfer & Mitigation • Risk Assessment Program	**Infrastructure** • Patch levels • Application Security • Cloud Security • Data Centre

Identify → Protect → Detect → Respond → Recover

WHY A CYBER RISK ASSESSMENT WAS SO IMPORTANT TO START WITH

MST Directors know that effective cyber risk management strategies cannot be implemented without applying suitably designed, configured and implemented risk management tools, techniques and methodologies.

The failure to identify, assess, and manage the major cyber risks facing their business would certainly and unexpectedly result in a significant loss of stakeholder value or possibly lead to a total failure should MST experience a cyber-attack. It's a case of when not if!

MST's directors and senior leadership realised that they must implement processes to effectively and efficiently manage all the organisation's critical cyber risks.

This could only be achieved using structured methodologies, appropriate tools and technology; and best practice implementation by suitably skilled specialists.

RESULTS FROM THE CYBER RISK ASSESSMENT

MST chose the NC3BRn risk management software platform "Cyber Risk Diagnostic tool" as the starting point for a step-by-step process that creates greater cyber exposure and clarity for the business and its stakeholders.

The NC3BRn platform provides MST with the ability to continuously monitor their cyber risk against international frameworks and standards e.g. ISO 27001 ,NIST etc. The cyber risk assessment allowed MST to focus on a review of all their IT Assets which were then mapped against all the threats applicable to their business.

Once this was completed MST looked at their current control environment and could clearly see what was lacking. This allowed for proactive and timeous identification of weaknesses in the control environment and automatic suggestions as to the next best control to implement. The reports produced through the process included practical guidance on the businesses specific cyber governance framework (CGF) that should be in place as part of an effective cyber risk management strategy.

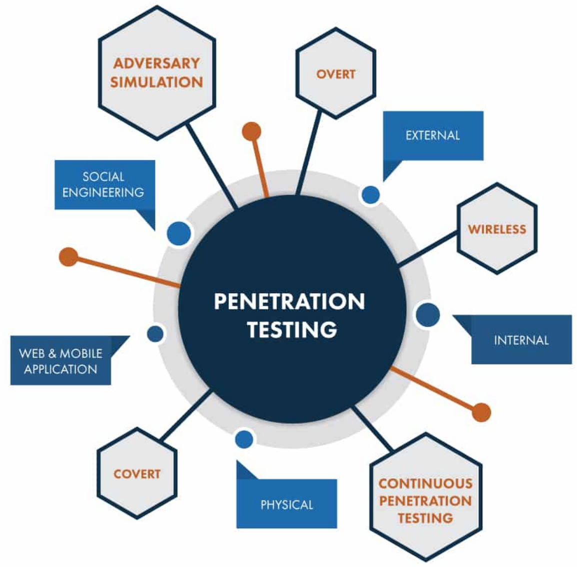
Both the tool and the reports generated on demand can be used to engage other company stakeholders into the process, such as chief information officers, IT security, Legal and HR. The board can now actively engage with and manage key risks effecting the business.

MST now has a detailed remediation roadmap and project plan allowing our board and stakeholders the opportunity to decide when and how to address the identified priority risks in a way that match our risk profile and appetite.

WHY MST CHOSE TO DO A VULNERABILITY ASSESSMENT AND PENETRATION TEST (VAPT)

MST wanted to prioritise key risks in their organisation and set up their own risk management process to allow them valuable insight into vulnerabilities in their network. MST wanted to identify and resolves vulnerabilities and misconfigurations before attackers had a chance to do so.

Once completed, MST would be aligned with globally accepted best practices and be POPIA compliant.



RESULTS FROM THE VAPT

MST received Short-term tactical fixes for immediate remediation for all outstanding vulnerabilities within the tested environments. A strategy was developed around long-term strategic measures that will proactively thwart any potential repetition of vulnerabilities discovered during testing as well as new ones.

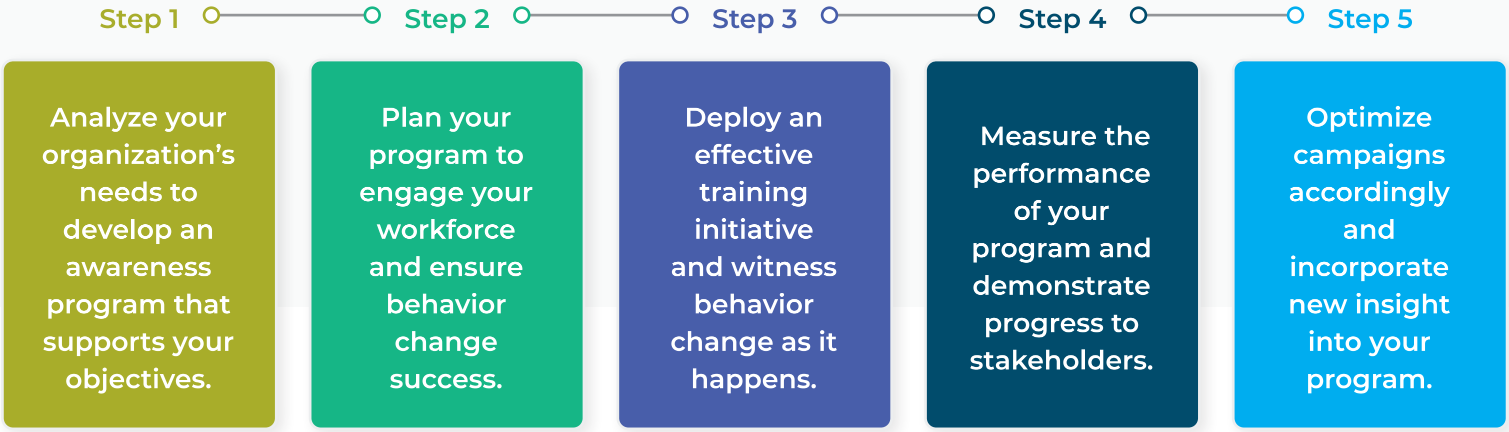
They received a robust set of conclusions and industry best practice recommendations based on real-world scenarios and tangible evidence of performance. There was a prompt engagement in remediation efforts and continued security assessments to ensure that consistent and ongoing security risk monitoring and security posture is reinforced.

A fully developed cyber resilience roadmap addressing all the issues uncovered and the strategic business objectives was developed and is being implemented.

MST realised that their staff are their greatest asset but (in a Cyber Context) may also be their greatest liability. By understanding the sophistication of social engineering and how hackers can manipulate staff through incredibly sophisticated and well-orchestrated human attacks, MST embarked on a defined and measured process of continuing Cyber education.

MST decide to implement the Terranova security Cyber training platform. The platform has been built around industry best practices and was founded by information technology education and security professionals with over 25 years of experience.

IMPLEMENT TRAINING WITH A PROVEN FRAMEWORK



Step 1 – Analyze your organization's needs to develop an awareness program that supports your objectives.

Step 2 – Plan your program to engage your workforce and ensure behavior change success.

Step 3 – Deploy an effective training initiative and witness behavior change as it happens.

Step 4 – Measure the performance of your program and demonstrate progress to stakeholders.

Step 5 – Optimize campaigns accordingly and incorporate new insight into your program.

Terranova Security products and services are the foundation for customising tailored security awareness programs to meet each Client's specific needs. Supported by a strong track record of skilled cyber resources and continuous innovation and new product development, the content also evolves as fast as email security threats, regulatory obligations, and social engineering-based attacks. Terranova is the exclusive training partner of choice for both Microsoft and Cisco.

Terranova has the most comprehensive multilingual library of cyber security awareness training to train your employees on best practices to recognise threats, protecting the organisation's data and reputation.

With this pedigree, the decision for MST was easy, and they implemented the Terranova training platform immediately.

CONCLUSION

“

The learning curve has been extensive, interactive and an eye opener for the entire business. We understand fully that cyber is not only an IT issue but a business one and as such we have all committed to following best practice.

We have now empowered out staff, IT department and shareholders with practical actionable tasks which continue to elevate our cyber posture and ensure that we follow a bespoke cyber resilience strategy. Our directors and shareholders receive understandable cyber and infosec reports which we can monitor and address depending on our risk priorities.

While we will never be “cyber safe” we have implemented remedial steps that ensure that we are at the leading edge of best practice (and beyond industry norms) and will ensure we are prepared to deal with any cyber incident that may occur in our business.

”

MST Resilience Case Study 2022

Reputation is everything!

For more information, please get in touch:

Barry C. Brown CPA, CITP | COO/CIO
T 770 995 8800
E bbrown@mstiller.com
mstiller.com

1960 Satellite Boulevard, Suite 3600,
Duluth, Georgia 30097