McAfee
An Intel Company

Security by Default:
Enabling Transformation
Through Cyber Resilience

FIVE STEPS TO BETTER SECURITY HYGIENE

Solution Guide

Introduction

Government is undergoing a transformation. The global economic condition, coupled with disruptive information and communications technology (ICT) capability and persistent malicious cybercampaigns, has forced a transformation in the service delivery and business model of government. This transformation is also forcing a change in how security is perceived and implemented throughout the organisation.

Security is critical to this business transformation strategy. In order for government to realise the value it can achieve through digital services, the resilience of the business and infrastructure systems must be assured. However, the infrastructure on which digital government services are deployed has become a complicated mix of multiple service providers and system integrators. While security services may be outsourced to these providers, government stakeholders maintain the responsibility for risk management and service assurance. Improving knowledge of key security challenges and necessary capabilities will help stakeholders manage their risk in the new service delivery model. It is important for any stakeholder to understand that managing risk is a dynamic balance spanning people, process, and technology.

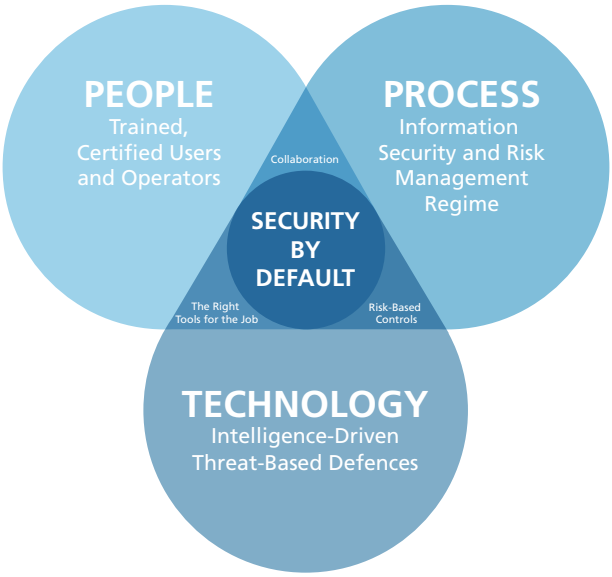

Figure 1. The concept of "security by default" aims to make baseline operational activities and systems start out in a "safe" state, rather than having security requirements addressed later, when they are less effective and more costly.

Throughout recent history, cybersecurity was viewed as a technology problem. Standard procedure was to simply update antivirus, encrypt data, and deploy firewalls to combat the security issues. While this often met security compliance requirements, our systems were still left vulnerable and service was not assured. The current situation in government will not allow such an approach to security anymore. The complexity of ICT systems, the broad and continuous threat landscape, and the desired outcomes of government for digital services necessitate a strategy of cyber resilience. But that strategy must be balanced across the people who use and operate the system, the technology used to secure it, and the processes used to monitor and respond. This strategy guide represents the core areas that must be addressed to enable cyber resilience in the digital systems of government.

Step 1: Develop an Information Security and Risk Management Strategy

A successful information risk management programme starts at the top of the organisation. Establishing a culture of risk management and accountability ensures that security becomes part of the business model and not an afterthought. Secondly, defining the information assurance framework formally establishes the security programme. This framework will include the policies and processes that form a secure, high-assurance foundation for the organisation.

A policy framework should include some of the following key components:

- Home and mobile worker.
- Acceptable use of government systems.
- Malware prevention.
- Privileged account management.
- Removable media.

A process framework will include some of the following key components:

- A training, certification and awareness programme for users, operators and security specialists.
- Secure configuration development and patch management.
- An incident management programme that includes monitoring and incident response processes.
- Penetration testing to assess security processes and control readiness.

Finally, incorporating cyber risk factors into business decisions regarding service assurance or new service deployment ensures that security becomes operational in the organisation.

Stakeholder Questions

1. Do we have the policies as recommended by best practice?
2. What is the required baseline user awareness training programme?
3. Do we have a recurring programme to educate users on new security requirements or threats?
4. What are the requirements for operator or security specialist training?
5. How do we test security monitoring and incident response processes?

Elements of an Information Security and Risk Management Strategy

PEOPLE	PROCESS	TECHNOLOGY
• Senior executives • Senior leaders • CIO • CISO	• Security awareness programme • User training and certification programme • Incident management programme • Readiness assessment programme • Compliance assessment programme	• Governance, risk, and compliance reporting dashboard • Executive dashboard

Step 2: Secure System Configuration Management Strategy

Employing baseline secure configurations of system architecture is an essential component of risk management. However, secure configurations are not static elements. They must be continually reviewed to keep up with threat conditions, new business functionality, or policy requirements. A process of design, test, monitor, and control is recommended as a secure configuration management process. Typically, the process starts with a system assessment to design the baseline configuration, additional security functionality required, and the change management process. Baseline configurations are usually available for commercial-off-the-shelf (COTS) operating systems and applications. However, custom web applications may need further testing to develop a secure configuration. The minimal additional security controls that will harden the baseline system against a variety of threat vectors should include the capabilities to: restrict removable media devices; conduct regular antivirus scans; and encrypt data at rest. However, web applications and databases may need additional controls above the baseline according to the system criticality or risk vectors.

Once deployed, the system should be continually tested for new vulnerabilities and monitored for unauthorised changes to the baseline or evidence of intrusion. Best practice recommends conducting regular vulnerability scans using automated tools that support open standards like the Security Content Automation Protocol (SCAP) to assess vulnerabilities. This open standard support allows for interoperability between assessment tools and faster exchange of information, including updates on items systems should scan for and assess. In addition to operating system vulnerabilities, it is important to test web applications and databases. These applications form a critical backbone of most digital government backend systems like ERP and CRM, but are usually not tested or monitored regularly as part of this process.

Stakeholder Questions

1. How does our secure configuration management process compare to best practice recommendations?
2. Do we test all components of our critical systems for vulnerabilities?
3. Do our tools and systems support open standards?
4. What additional security controls are in use on our end-user devices?
5. Do all mobile end-user devices with sensitive data use encryption?

Elements of a Secure System Configuration Management Strategy

PEOPLE	PROCESS	TECHNOLOGY
• System administrators • Application developers • Penetration testers • Compliance audit	• Baseline design • Application code review • Vulnerability assessment • Compliance assessment • Change control assessment	• Vulnerability scanner • Web application scanner • Database application scanner • Security incident and event management (SIEM) • Antivirus • Host device control • Data-at-rest encryption

Step 3: Establish an Anti-Malware Strategy

Malware is the tool of choice for any hacker and has many vectors into an organisation. However, most organisations mistakenly equate anti-malware with antivirus. As malware becomes increasingly sophisticated and the attack surface increasingly diverse, a successful anti-malware strategy must include a dynamic capability to prevent, detect, and respond to limit the impact of malware as an attack vector. A layered defence to malware starts with the user. Although layered defence most often addresses technology, users and system operators must be trained to recognize attack methods, such as phishing, and understand where to report suspicious activity. Since many successful attacks often target a specific user, training is an essential anti-malware control. A recurring and accountable user security awareness programme is the first and last line of defence.

The end-user device's baseline security configuration already includes antivirus as a first layer of defence. Hardening devices or servers with additional security capability beyond antivirus, such as application whitelisting and reputation intelligence, will provide an effective defence at the host layer, even against malware that uses zero-day exploits. Security and change events generated at the host should be centrally collected, monitored, and analyzed by the security operations and intelligence centre (SOIC) to detect potential incidents.

Although application whitelisting and antivirus are effective prevention tools, malware is a multi-stage attack utilising several vectors into and out of the protected network. A comprehensive anti-malware strategy must include a network capability to recognize malware behaviours on the network and to protect devices that may not support host-based security controls. Since the most common delivery and command vector for malware is via the web, it is recommended to deploy web content anti-malware inspection at the Internet perimeter to better protect end-user devices or detect evidence of malware behaviour already inside the network. By employing a web gateway with strong anti-malware capability, such as sophisticated content emulation, botnet identification, and reputation intelligence, organisations increase not only their resilience against malware, but also their agility to adopt new enabling technologies. As with host security events, events from network anti-malware devices should be centrally collected, monitored, and analysed by the SOIC to detect potential incidents.

As mentioned, a comprehensive anti-malware strategy involves a people, process, and technology approach. One of the key processes in an anti-malware strategy is to identify, validate, contain, and respond to security incidents. When a suspicious event is identified, security analysts in the SOIC must rapidly validate the malware, uncover its characteristics, and find affected hosts in order to contain the impact, such as data loss or further compromise. Having direct access to automated malware analysis tools and real-time data sources will greatly increase the speed of analysis and reduce the impact of malicious activity.

> "Most organisations mistakenly equate anti-malware with antivirus."

Stakeholder Questions

1. What is our multi-layer anti-malware strategy? Does it include a people, process, and technology approach?
2. Do we employ application whitelisting as additional security on end-user devices?
3. Do we employ automated analysis and real-time data sources in the SOIC?
4. What is the strategy to prevent malware on the network?
5. Do we monitor for and respond to potential security incidents centrally?

Elements of an Anti-Malware Strategy

PEOPLE	PROCESS	TECHNOLOGY
• Policy awareness training • Incident reporting procedures • Incident handling procedures • Threat awareness training	• Breach monitoring and response • Malware and forensics • Incident handling process	• Application whitelisting • Antivirus • Web content inspection • Reputation intelligence • Malware sandbox • SIEM

Step 4: Network Security Strategy

The role of network security is expanding and changing with the expansion of digital services in government. Traditionally, network security devices functioned as traffic cops governing which network addresses can pass or which protocols can traverse the Internet perimeter. While still providing that function, the goal of the network security strategy is to deny, delay, and disrupt the ability of an attacker to get in and move around on the protected network systems. To enable this strategy, network security devices have evolved from controlling addresses to identifying and controlling application access across multiple security zones within the enterprise.

Dividing the network into logical security zones requires different checkpoints for an attacker. Typically, one of the internal security zones is the consolidated or shared services datacentre. An effective datacentre network security strategy requires an application layer firewall for controlling application access and an intrusion prevention sensor to protect the sensitive applications from vulnerability exploitation. Other potential network security zones include partner and cross-domain network interconnections. Each of those connections requires an application firewall to control access. The risk of vulnerability or malware exploitation is low across these perimeters. The greater concern is the access to or loss of sensitive data to unauthorised business or coalition partners. Best practice recommends a network data loss prevention solution be deployed and monitored at these perimeter locations.

The adoption of cloud services presents unique challenges for traditional perimeter security solutions. While an application-layer firewall provides granular traffic control at the Internet perimeter, many applications are exposed to external cloud services through application programme interfaces. Today, on-premises deployment of a centralised service gateway is recognised as the best practice deployment pattern for the application-to-application, web-based service interaction models. A service gateway enables the enterprise to develop a standards-based policy enforcement point that is integrated with internal identity management and auditing/monitoring infrastructure.

Stakeholder Questions

1. Does our network security strategy include granular application identification and inspection capability?
2. What are the various security zones in our internal organisation and how are they protected?
3. Does our perimeter network security strategy include granular web application controls and proxy capability?
4. How do we control access to cloud services, especially API content security?
5. What is our datacentre network security strategy?

Elements of a Network Security Strategy

PEOPLE	PROCESS	TECHNOLOGY
• Data awareness training • Network usage policy • Certified security system operators	• Data readiness • Identity management • Network controls monitoring • Data loss monitoring	• Intrusion prevention sensors • Application-aware firewall • Network data loss prevention • Cloud services gateway • SIEM

5. Security Monitoring and Intelligence Centre Strategy

With the sophistication and persistence of malicious cyberactivity combined with the complexity of security information, detecting or anticipating a security breach requires an organisational monitoring and intelligence strategy, trained specialists, and a 24/7 security monitoring and intelligence centre. The functions of this centre usually comprise three main areas: breach response, readiness assessments, and intelligence. This guide will focus on breach response as the common area.

Breach response is the process of identifying, validating, containing, and mitigating a cyber incident. The effectiveness of this process depends upon:

- Threat intelligence on attackers' methods and infrastructure.
- Sensor grid comprised of network, application, host and content monitoring tools.
- An automated analysis capability that can address sophisticated malware techniques.
- A centralised data collection strategy.
- Real-time data mining and pre-planned response capabilities.

Identification is the first step in the process, and often where organisations fail. Deploying an intelligent sensor grid that exposes the right information for analysis is the key first step. For example, we understand from threat intelligence that targeted attacks usually start with a download of infected PDF file from the web. A good technique for detecting advanced attacks starts with capture of suspicious PDF files at the network perimeter. A security monitoring and intelligence centre analyst would then validate the file is malicious through automated analysis tools, such as a malware sandbox. If confirmed to be malicious, the analyst would use real-time response and data-mining capabilities to contain and mitigate the attack.

To sum up, an effective breach response strategy should employ a sensor grid, automated malware analysis, and centralised data mining and control capabilities. By harnessing these systems to work together, you can massively increase the speed of response.

This process requires several different types of data for validation. Centralising this data inside a security information and event management (SIEM) system will facilitate rapid data mining for both identification and validation. Most organisations will collect network traffic, security events, server and device events, and user behaviour, as the foundation of the breach monitoring capability. However, best practice recommends extending the data sources to include database application events, web proxy logs, identity management, external intelligence context, and DNS logs. It is essential that the SIEM system scales to handle those additional high-volume data sources while still enabling rapid data retrieval for reporting or analysis.

All of this analysis capability produces a lot of intelligence on attacks happening locally to the organisation. Intelligence capture must be part of any monitoring and response strategy. It is critical to integrate the local intelligence back into the process for future context.

Stakeholder Questions

1. Do we have a 24/7 security operations monitoring and intelligence centre?
2. What is the data strategy that supports our breach response process?
3. Do we employ data mining technology to find and validate a breach?
4. What is the sensor grid strategy that supports our breach response process?
5. Do we integrate external and capture internal intelligence as part of the breach prevention strategy?

Elements of a Security Monitoring and Intelligence Centre Strategy

PEOPLE	PROCESS	TECHNOLOGY
• Malware analyst • Forensic analyst • Incident handler • Data and storage architect • System administrator • Intelligence analyst • Security architect	• Detection use case development • Breach monitoring • Incident response and reporting • Threat assessment • Readiness monitoring • Penetration testing • Intelligence collection and exchange • Data strategy development	• Malware sandbox analysis • Intrusion prevention sensor • External reputation intelligence • SIEM • Multiple security event data sources • Multiple network or host data sources

Take Action

This brief is a tool to educate government stakeholders on cyber resilience strategy issues. With this foundational understanding of how to create a secure by default environment, you should be ready to move ahead.

1. Schedule a strategic consultation session to understand how McAfee can help formulate a strategy with your organisation.
2. Engage key operational and security personnel in a conversation with McAfee about implementing these strategies.
3. Review our technical guides at www.mcafee.com/publicsector to see how McAfee can implement these strategies.
4. Review additional information on www.mcafee.com/publicsector to see how McAfee enables cyber resilience across government organisations and agencies.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60228sg_public-sector_0613_wh