mti™
Managing Data Securely

steps to CYBER SECURITY

A Guide to Implementation

+44 (0)1483 520 200 | ukinfo@mti.com | mti.com

Contents

Foreword

In January 2016, the UK government relaunched its '10 Steps to Cyber Security' guide. Originally released in 2012 by Communications Electronic Security Group (CESG), now part of the National Cyber Security Centre (NCSC), the information arm of GCHQ, the guide offers practical guidance on the steps that organisations can take to improve the security of their networks and data.

On the back of this relaunch, **GCHQ said it continues to see real threats to the UK on a daily basis, and the scale and rate of these attacks shows little sign of abating.** Cyber-attacks have become so common that, for many companies, it's not a question of 'if', rather 'when.'

Every day thousands of IT systems are compromised. The motives vary but most commonly, they are attacked to steal money or commercial secrets. In fact, never has the need for robust and rigorous cyber security been greater. Today, an organisation can lose £50 million in a hack and barely an eyebrow is raised, illustrating just how commonplace major cyber hacks have become.

The Ponemon Institute's 2015 Cost of Cyber Crime Study: United Kingdom determined that the average annualised cost of cyber-crime to large organisations in the UK is now £4.1 million per year, a year-on-year increase of 14 percent. These findings were based on 39 benchmarked organisations in the UK. Each had a minimum of approximately 1,000 connections to the network and enterprise systems.

However, **damage from cyber-attacks isn't just limited to financial loss; reputational damage can be even more devastating, destroying a company's credibility and leading to a loss of business.**

The modern cyber threat landscape is such that all sensible organisations must accept the inevitability of a cyber-attack and prepare accordingly. The UK government's '10 Steps to Cyber Security' offers a blueprint to help guard against it and ensure robust and rigorous defences.

Today, there is a much greater awareness of the importance of IT security, but it's taken a long time to arrive at this point, and some serious cyber-attacks along the way.

The bottom line is that cyber security is not an IT issue, rather it's a strategic risk management issue and IT is simply the means to enable this strategy. In an age that is defined by the ubiquity and economic power of the Internet, cyber security is an absolutely vital foundational step for any organisation.

Andrew Tang, Service Director – Security, MTI

Introduction

The government guidelines offer practical insight into key areas of information security ranging from implementing an information risk management regime to home and mobile working. The guidelines cover ten areas:

- Information Risk Management Regime
- Secure configuration
- Network security
- Managing user privileges
- User education and awareness
- Incident management
- Malware prevention
- Monitoring
- Removable media controls
- Home and mobile working

This paper looks at each area, spells out what exactly it means and explains how you can successfully address the issues raised.

1 Information Risk Management Regime

For any security regime to be truly successful, it must be sanctioned and driven from the executive board level to ensure it sweeps down through the organisation and is taken seriously. This is the foundation for robust security practices.

It is, however, relatively rare to see a board level executive with responsibility for security. Typically, this falls to a CIO, or someone who has authority rather than advisory powers, often just below board level.

The government guide quite rightly suggests that cyber risk should be addressed regularly at board level. This would be a significant step and one that shows cyber security is being taken seriously.

Time and again we see instances where cyber security isn't taken seriously and the consequences for the companies involved can be huge. In the US, **Target, a national retailer, suffered a serious breach in which 40 million credit and debit card details and 70 million customer records were stolen[1].**

The breach had a devastating effect on reputation and revenues plunged by a staggering 46 percent[2] in a quarter-on-quarter comparison.

46%

In the UK, TalkTalk's[3] CEO Dido was also under pressure following a breach of a customer database. The company had clearly learned lessons from other major breaches and didn't attempt to confuse the issue. It quickly came clean about the breach. It was, however, quite clear the CEO was out of her depth in talking about the breach and whether data was encrypted or not, which led to a gale of media criticism.

One way to get the interest of board members is to speak to them in a language they understand such as potential reputational damage, the impact on revenues, loss of customers and other strategic issues.

ico. Information Commissioner's Office

With the Information Commissioner handing out fines of up to £500,000 for leaking customer data, it is not a subject to take lightly. These points may seem dramatic however it reflects the seriousness of cyber-breaches.

Identifying vulnerabilities that can lead to a breach is achieved by carrying out a risk assessment. In fact, this is the first essential step in developing and implementing a security policy. A risk assessment requires a thorough analysis of a company, its assets and its value. Typically, this is intellectual property and customer details.

It's important to ask the right questions when dealing with cyber security. Where is data stored? Is the database secure? Is the website secure? Where does data travel in and out of the network? What is the BYOD policy? Are software updates carried out regularly? Who has responsibility for network security?

Once you have the answers to the above questions, a security policy can be developed along with an Information Risk Management policy. This will outline any areas of responsibility, compliance requirements, incident management, monitoring, reviews and so on.

A lifecycle approach is also essential to risk management, where policies undergo regular review to take account of new developments. For instance, if the organisation is beginning to incorporate 'Internet of Things' technology into operations, this needs to be taken into account, with vulnerabilities assessed and security enabled.

2 Secure Configuration

Once a security policy has been agreed, areas of vulnerability have been outlined and the values of different types of data and responsibilities are confirmed, the next step is to ensure the existing technology and infrastructure is secure.

As systems become more complex due to additions of new software and hardware, vulnerabilities can appear quicker.

Secure configuration is a question of maintaining control as the IT environment evolves. Ensuring you know what applications end users are downloading and that a comprehensive update strategy is in place to patch software is crucial.

When users download and install software, it can conflict with existing applications and create vulnerabilities as unpatched software presents an open door for hackers.

It's worth remembering that hackers and cyber-criminals put enormous effort into identifying and exploiting software vulnerabilities. In fact, there is a vast underground network operating largely on the dark web dedicated solely to developing malware that exploits vulnerabilities and selling it to other hackers.

One of the difficulties for IT administrators is managing all of the applications within an IT environment. Given the size of some IT operations, it can feel like, and often is, an impossible task without expert guidance and the right tools.

The government guidelines quite rightly point out that, "Without an awareness of vulnerabilities that have been identified and the availability (or not) of patches and fixes, the business will be increasingly disrupted by security incidents."

A salient point and a nightmare for any CIO is a major system breach, which happens as the result of unpatched software or the exploitation of insecure system configurations.

Adopting a holistic approach will help secure configuration and also urge endpoint standardisation. This will help simplify and manage what can sometimes feel chaotic. Centralising the management approach also ensures industry best practice is maintained.

There are a number of unrivalled benefits to this approach. Firstly, it ensures endpoints and applications are not only patched, but also properly configured. When implemented correctly, it also carries out assessments on software flaws and configuration vulnerabilities, whilst at the same time delivering rapid remediation, continuous validation and policy compliance reporting.

Secondly, everything that is happening across the network, from software downloads to new endpoints that are added can be seen. As a result, potential vulnerabilities are flagged and standards-based remediation is applied, ensuring optimum security.

3 Network Security

The development and ubiquity of the Internet has been a great thing. It has opened up the world, making previously closed shops available on a global scale. However, as the Internet grows, so does cyber-criminal activity. It's therefore imperative to have a robust and rigorous network security solution in place.

A critical first step is the need for a firewall on the perimeter of your network that carries out deep packet inspection, monitoring the traffic coming into the network. This needs to be fortified with robust antivirus which can also filter websites and inbound emails to guard against malicious links and phishing attacks.

You need to be looking out for malware that is attempting to get into the network, emails that have Trojans hidden in them, websites with poison links and any other network traffic that may be harbouring malicious software. It's important to remember, though, that the landscape isn't fixed, it's constantly changing as new attack methods are developed and malware mutates to avoid detection.

Protecting the environment is made more complex by distributed enterprises that have branch offices and remote or roaming users, or data centres that use technologies like virtualisation and the cloud.

The Communications Electronic Security Group guidelines say you need to: **"Filter all traffic at the network perimeter so that only traffic required to support your business is allowed, and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an attack."**

For any CIO or IT administrator, these are basic first steps. The approach taken will, however, be determined by the IT environment. When protecting the perimeter, you need to consider that your network is full of applications that a port-based firewall fails to identify or control.

File sharing, social networking, personal email and streaming media are just a few of the applications that can evade your firewall by hopping ports, using SSL, or non-standard ports. Blocking these applications may impact on the business. As such, you need an approach to create effective firewall-control policies that extend beyond the traditional 'allow or deny' approach.

Similarly, **if you're protecting a virtualised data centre, you'll need to consider how to enable and protect applications moving across the cloud,** how to isolate applications and how to eliminate the security lag as your cloud environment changes.

If you wish to safeguard a distributed environment, another approach is required. It's common in these environments to see clients with smaller branch offices, employees working remotely from home, and roaming users. In fact, users often move from one location to another within a day - while it's great for productivity, it can lead to dangerous inconsistencies and IT compromises.

Although each environment requires a different approach, each essentially has the same goal, to optimise visibility, increase control and eliminate policy configuration gaps.

4 Managing User Privileges

Managing user privileges is an important aspect of comprehensive information security. Ideally, employees should only have access to the data and systems necessary to carry out their role. The problem is that unmanaged privileged accounts can lead to all sorts of problems for a business.

Think of a privileged account as an access-all-areas pass to confidential business data and systems, allowing users to grant broad access rights that often go far beyond what is needed for that job function. Monitoring the actions of users is therefore paramount for security and compliance.

However, despite this, monitoring is not something that is standard practice. **Cyber-criminals are only too aware that many privileged accounts often go unmonitored, unreported and as a result, are unsecure.**

They understand that access to a privileged account provides the ability to control the organisations resources, disable security systems, as well as access to vast amounts of sensitive data. The damage done proportionately can be very severe.

If cyber-criminals gain access to a privileged account, they can basically jump over security so whether data is encrypted or not becomes irrelevant.

Privileged account users can include third-party providers, cloud server managers, systems administrators, application or database administrators, select business users such as senior-level executives and social media. Compromising any of these accounts can create considerable problems.

The best practices dictate that privileged accounts should be incorporated into an organisation's core security strategy. This means that controls need to be put in place to protect, monitor, detect, and respond to all privileged account activity.

There are several ways to control privileged account activity. Some organisations choose to deploy a strategic solution across the entire enterprise, while others take a 'stepped' approach that involves looking at the most vulnerable points first.

Starting with securing privileged credentials and then moving to monitoring the accounts, once secured, enables the implementation of the underlying infrastructure. Using analytic algorithms can also help reveal previously undetectable malicious privileged user activity as it monitors behavioural data.

Introducing layered security such as encryption, tamper-proof audits, and data protection can also help with protection of accounts, especially when used in conjunction with other methods. Multiple authentication methods assist in keeping your files and data protected from both internal and external threats.

Monitoring the actions of privileged accounts is fundamental to security. Do not let protection let you down.

5 User Education and Awareness

Education provides the building blocks for good security. User education is about raising awareness about the risks and dangers that can arise from a slack approach to security. This can be anything from bringing USB sticks into the workplace and plugging them into computers, or a lack of understanding about social engineering and phishing.

Within this context, the weakest link in the business can be employees that lack IT security knowledge. Leading-edge technology can be irrelevant if employees are not aware or educated on a comprehensive security policy.

Spear phishing attacks, for instance, can be particularly damaging. A few years ago, RSA, a high profile security company, and its cryptography keys were compromised in spear phishing attack[4].

The emails contained a malicious attachment that was identified in the subject line as 2011 Recruitment plan.xls. One of the recipients eventually opened the infected spreadsheet that led to the breach. In this respect, education is crucial.

None of the recipients were people who would normally be considered high-profile or high-value targets, such as an executive or an IT administrator with special network privileges. However, that didn't matter. The malware had been unleashed. Once a spear phishing email makes it through filters and other similar technologies, the user element really comes into play, which is what the hackers were depending on.

When educating users, awareness is only the first step. Training must also be used. It provides people with a fixed body of knowledge which they can be tested on.

Training can take place in incremental steps or be focused on specific business requirements. It doesn't need to be a sweeping one-size fits all programme, it can be bespoke, targeting a specific department or focusing on remediating certain behaviours.

One thing is certain, a trained and educated workforce will dramatically reduce the chances of your organisation ending up as headline news or seeing its valuable customer information for sale on the dark web.

6 Incident Management

An incident management strategy is vitally important to contain damage, should it happen. In fact, IT system breaches need to be considered within the context of disaster recovery and business continuity, as well as mandatory reporting requirements.

One of the best ways to develop an incident management strategy is by using existing standards. **The ISO 27000[5] family of standards helps organisations keep information assets secure.** Specifically, the ISO/IEC 27001 is the best known standard outlining the requirements for incident management. It covers people, processes, and IT systems, all of which are viewed through the lens of risk management.

These standards help organisations manage the security of its assets, whether it's financial information, intellectual property, employee details, customer details or third party information by providing a systematic approach.

The ultimate goal of ISO 27001 is ensuring security requirements are met and as such it incorporates incident management as a central component.

An incident management strategy starts with the identification of incidents, typically with users logging them and also automatically generated incident logging based on pre-established conditions.

Incidents then need to be categorised to enable easy classification. In turn, this informs prioritisation, such as: the effect an incident has on business, whether it needs to be dealt with urgently or whether can it be managed at a later stage.

When an initial identification has been made and the incident categorised; diagnosis, escalation, investigation and resolution need to take follow. While some of these processes can be automated some are also dependent on human processes and intervention such as investigation and diagnosis.

Depending on the incident, this often involves forensics. This is where a back track process takes place so the cause and location of the incident can be established. This is important because a hacker can plunder a customer database and have credit card or banking and personal information up for sale before the company is aware anything has happened. As such, it's important to be able to detect the path of the attack and trace it back to a source, date and time.

In summary, an incident management strategy needs to be a central component in a wider disaster recovery strategy. The point of incident management is that it enables you to effectively identify and manage breaches.

7 Malware Prevention

The scale of malware is enormous. **Approximately 250,000 new malware sites are brought online every day[6].** While the majority of these are only alive for around 24 hours, they can cause enormous damage.

This is particularly true when malicious sites are combined with different attack methods such as phishing or pharming or even search engine manipulation.

All it takes for malicious malware to end up in your network is an employee to fall for a phishing email or clicking on a poison link and then being redirected to a website where a Trojan is implanted into the network.

Malware can lead to blackmail, the deletion of entire databases, key loggers that record every finger tap across a keyboard, backdoors that are used to implant malware, rootkits that provide full access to a system and passwords stealers.

As malware has been around for such a long time, everyone is familiar not only with the damage it can cause, but also its ubiquity. As a result, there is widespread understanding that it needs to be guarded against, which is positive.

The most effective way of doing this is via robust and rigorous antivirus at the firewall. Antivirus needs to dovetail with other defence methods such as real-time threat detection and forms of detection that don't just rely on detecting virus signatures. This is because host and client machines also need protecting.

While signature detection is important to block the hundreds and thousands of malware variants that swarm the Internet, it's not enough to detect newly-released malware, so called zero-day threats.

As more Internet traffic becomes encrypted via the HTTPS protocol, the need for layered malware protection becomes more acute.

It's possible to use technology that not only sends an alert that an unknown file has entered your network, but also informs you whether it reached a computer, if it executed, what it did, when it ran, if it spread or deleted itself and so on. If the file is malicious, you can automatically stop it from executing. This enables you to rapidly prioritise alerts, investigate events, and remediate incidents.

This holistic, layered approach recognises that malware infections are, not only, too common, but the enterprise needs protecting across the range of its systems. From the perimeter firewall to endpoint devices, protection is needed at every stage.

8 Monitoring

Monitoring IT systems is central to the protection of an organisation, however it must be comprehensive.

This means looking at everything from the networks, servers, desktop computers as well as host intrusion detection systems, prevention solutions, and wireless intrusion detection.

In the past, it was a widely held belief that system monitoring was not a core requirement for operational effectiveness.

However, the dramatic and sustained surge in cyber-attacks[7] and the threat from insider data leaks, presents this argument as redundant. The need to protect sensitive data, whether it's customer information, financial records or intellectual property has never been more pressing. **At its core, monitoring essentially needs to track activity as well as raising red flags if anything out of place happens.**

There are a number of ways to approach this. We recommend centralised technology platforms that detect threat activity as these provide the security team with the context and insights needed to minimise the potential fall-out.

It's not just a question of looking out for malware; it's a question of having full insight into the IT estate and all its component parts. It needs to be comprehensive, given that some threats are multi-vector advanced persistent threats carried out by external attackers, while others arise from malicious or accidental behaviour by insiders.

A business needs to be able to use data loss prevention tools to detect even a partial fragment of sensitive data on a network endpoint, as well as guarding against data loss in the cloud and on premise.

Detailed analytics help you understand what is normal organisational behaviour as well as helping to highlight when something or someone deviates from the norm.

Preconfigured policies are also important in that they allow you to get up and running quickly and more importantly, effectively. The importance of monitoring data and human behaviour can't be overstated, especially as it can give you an early warning system that flags up if something is amiss.

9 Removable Media

Removable media is anything that can be brought into an organisation and plugged into a computer, ranging from a USB stick to external memory, smartphones, tablets, iPods, Bluetooth devices, recordable CDs and DVDs. It also includes wearable devices such as smartwatches, which are gradually becoming more popular.

Some people in the workplace may use a laptop to charge their smartphone or transfer files using a memory stick because it contains something they are working on. However, irrespective of what it is you're plugging in, there are dangers attached when inserting a USB into your laptop. Firstly, there's the risk of the devices containing malware and secondly, there's the danger that sensitive data can be downloaded and stolen.

An attack on an Iranian nuclear plant in 2013[8], illustrates the tremendous damage that can be wreaked from a small memory stick. Stuxnet centrifuges was essentially programmed to spin out of control and self-destruct. While this was a case of state-sponsored cyber espionage, it shows how removable media can be used to penetrate even the most comprehensive of security systems. It's therefore essential not to overlook removable media controls when looking at cyber security.

In the corporate sphere, the risks of information theft, data loss, and malware can all lead to reputational damage and financial loss for a company. If you have any doubt about the consequences of serious data loss, consider the case of US retailer, Target. [9]It was the subject of a hack in which millions of customer records were plundered and as a result, its revenues plunged by over 40 per cent.

Safeguarding against loss via removable media should ideally be planned when a security policy is being developed. As removable media in the workplace is now all too commonplace, and is one of the highest areas of vulnerability, it should be addressed as a matter of urgency.

Even if your network is locked down to the point of disconnecting it from the Internet, that doesn't prevent someone from copying sensitive data onto a CD-ROM, or to a USB memory drive and walking out the door with it.

Removable media controls fall under data loss prevention and as a result, there is a raft of technologies designed to help protect the removable devices. The fast-paced business environment of today requires employees to have anytime-anywhere access to corporate data and business applications, therefore putting the block on removable media may seem draconian and counter-productive.

However, it can be managed. It's possible to protect critical data from coming into and leaving the company via removable media with tools that monitor and control data transfers from desktops and laptops, irrespective of where users are and even when they are not connected to the corporate network.

Specifying which devices can and cannot be used, defining what data can and cannot be copied onto allowed devices and restricting users from copying data from specific locations and certain applications will help when managing devices.

Endpoint encryption for removable media is also another effective approach. It allows the encrypted device to be used on any machine without installing any software or requiring administrator privileges. It also allows encrypted files to be saved or edited safely, which ensures user flexibility is also maintained.

Remember, policy is essential. Identifying removable media devices, nailing down required actions and outlining the steps that are needed to ensure continued business flexibility will help protect your sensitive data.

Home and Mobile Working

Mobile working is an established fact of life today, whether you're accessing corporate data on the move or connecting to the company network from your home. Mobile devices now make it easier for employees to do all they need irrespective of geographical location.

While the mobile revolution provides flexibility for employees, it also brings risks, one of which is the simple physical loss of equipment, such as a laptop left on a train, or a smartphone left in a taxi. **In short, the ability to access all documents from a single location means that, should the device end up in the wrong hands, its security can be compromised.**

Should you happen to find yourself in a situation whereby your device goes missing, do not panic. Laptop lapse can easily be dealt with by encrypting hard drives, enabling remote access to wipe data and also by using extremely robust passwords.

A more immediate danger, however, are sophisticated exploits such as mobile botnets, where multiple smartphones can be infected with a virus or Trojan type software. This can result in a network of phones being programmed for malicious activity, such as stealing credit card data or malware burrowing into a corporate network. As mobile computing becomes increasingly commonplace, hackers are also increasingly drawn to it.

In terms of home and mobile working, organisations need to secure and manage operating systems in a world of mixed-use devices, while at the same time incorporating identity, context, and privacy enforcement to set the appropriate level of access for enterprise data and services.

Organisations need to address three areas:

- *Device management*
- *Application management*
- *Content management*

Device management - organisations need to be able to secure and manage a diverse range of mobile devices, automatically enable enterprise settings such as Wi-Fi and VPN, as well as providing end-users with secure access to corporate email.

Application management - business should aim to deliver, secure and when appropriate, retire mobile apps. This provides IT with the ability to manage the application life cycle from making applications available to employees, securing applications on the device and when necessary, containerising corporate apps to keep them separate from personal apps.

Content management - this is the ability to enable end-users to securely access and manage enterprise documents that are kept in different content repositories, whether on-premises servers or in the cloud. It's also important that corporate email attachments are encrypted. Ideally, users should also be able to securely browse corporate Intranet content without the need for a device-wide VPN.

Policy guidelines also need to be in place in order for a business to dictate actions. For instance, if a mobile device falls out of compliance, IT can define remediation actions that will either notify the user of policy violations or remotely wipe corporate information.

In addition, stating how an employee should connect to the corporate network can also help with security. Connecting to a corporate network via secure socket layer virtual private networks alongside a two-factor authentication for identification will also ensure privacy and protect corporate data.

Conclusion

Protecting key information assets is of critical importance to the sustainability and competitiveness of businesses today.

The UK government's '10 Steps to Cyber Security' outlines the practical steps business can take to improve the security of their networks and the information carried on them.

By following these guidelines, companies will benefit from managing risks across their organisations, be able to draw on senior management support, implement risk management policies and processes, and create a risk awareness culture.

MTI is a global provider of IT security solutions and services. Our Datacentre, Managed Services, and Security practices work together to deliver tailored services and solutions that help to solve real business challenges for our clients.

We engage with staff at all levels of an organisation – from back office, to boardroom to really understand your business, as well as your goals, objectives, and strategy.

We then leverage the expertise that we have gained over the last 25 years to provide guidance, and to help your organisation innovate, grow, and drive positive business outcomes within a robustly secure framework.

References

1. *Bloomberg Business Review, March 17, 2014*
2. *Wall Street Journal, February 26, 2014*
3. *Guardian, 6 November, 2015*
4. *Wired, August, 2011*
5. *www.iso.org*
6. *Institute of Legal and Finance Management*
7. *Symantec 2016*
8. *Business Insider, November 20, 2013*
9. *International Business Times, September 21, 2015*

Contact MTI Today

Managing Data Securely

MTI - Global Solutions and Services Provider

Datacentre - Managed Services - Security

to find out more, please visit www.mti.com

Call us on +44 (0)1483 520 200

Email us at ukinfo@mti.com

MTI Technology Limited, Riverview House, Catteshall Lane, Godalming GU7 1XE

10 steps to CYBER SECURITY