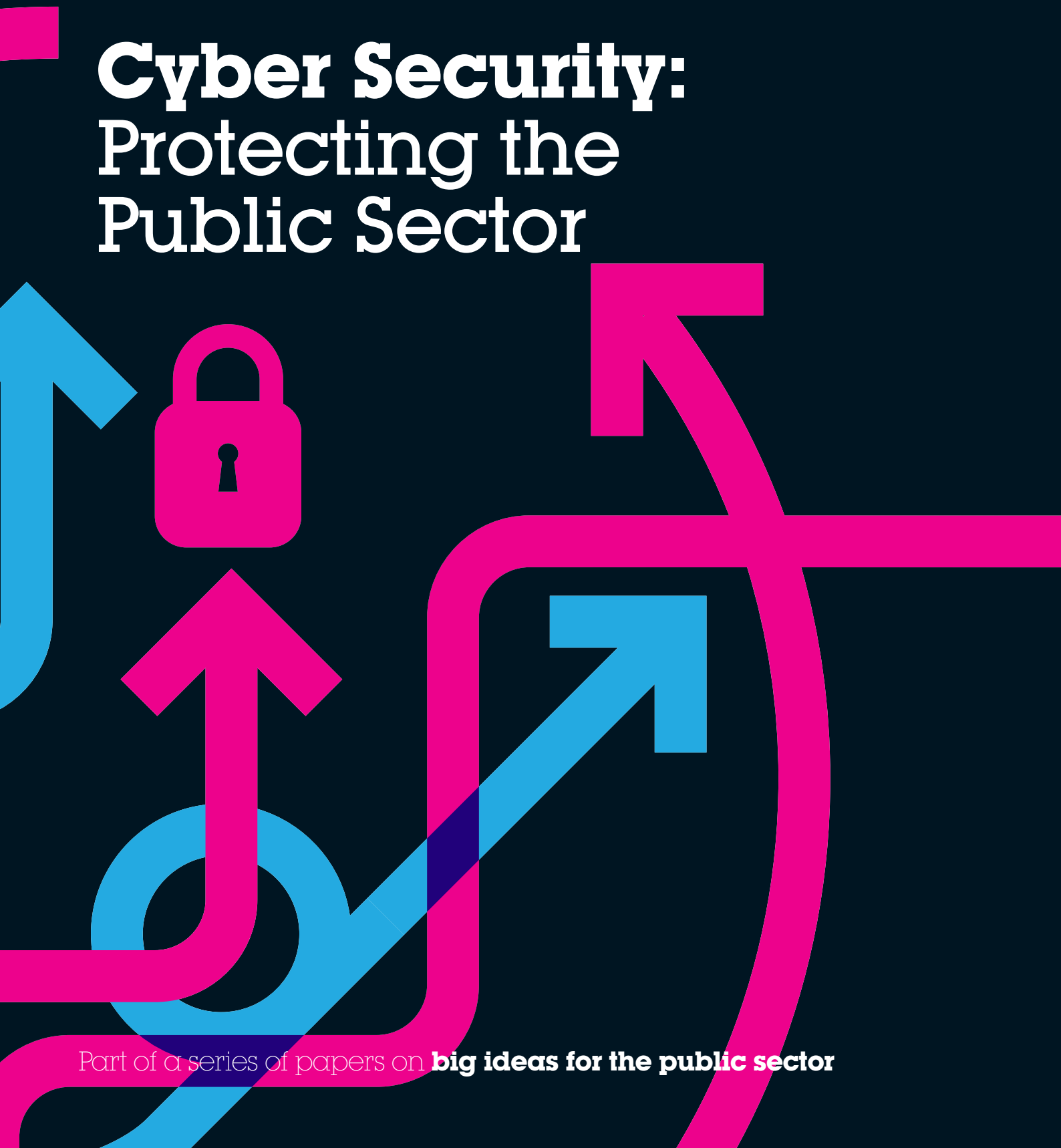
Public Sector

IBM

Cyber Security: Protecting the Public Sector



Part of a series of papers on **big ideas for the public sector**

Cyber threats represent **a real and significant danger** to the UK, its citizens, businesses and its overall economy. It is essential that we maintain confidence in services that are critical to economic well-being and sustain everyday life. **Tackling cyber security is challenging and the threat is rapidly evolving and expanding.** Cyber security is more than any one individual step; it is a process: **Learn. Monitor. Analyse. Decide. Respond.** These five steps could be vital to cyber security in the UK public sector.


62%
of managers believe cyber threats are an increasingly serious risk to business[1]

THE THREATS

In December 2009 Google detected "a highly sophisticated and targeted attack" on its corporate infrastructure, dubbed "Operation Aurora". It originated in China and targeted Google and at least 20 other organisations.[2]

In July 2010 a computer worm known as Stuxnet was discovered that targeted industrial software and equipment controlling and monitoring a variety of industrial processes. Named Stuxnet based on some keywords found inside the program, this worm looks for a very specific environment before enabling its payload. Most of the systems affected by the worm were in Iran, leading to speculation that this too may have been an attack with governmental support if not origins.[3]

Early in 2011 officials at the International Monetary Fund revealed that it had been targeted by a sophisticated cyber attack[4] – a threat that was considered so serious, the World Bank severed the computer ties through which the two organisations shared information.

In June 2011 a black-hat hacker group known as LulzSec (or "Lulz Security") targeted the website of the CIA in the US using a denial-of-service attack[5]. This was the latest in a string of similar attacks against a range of government and public sector bodies.

While there is ample data on activity, there are few statistics and little trend information about the motives for cyber threats today.

According to LulzSec, for example, they were not doing it for political reasons or financial gain; they simply did it "for the lulz" (laughs) and publicity. According to IBM research[6], a rise in "hacktivism" can also be observed across the globe, where attackers are no longer motivated simply by recognition or financial gain, but also by political reasons.

And attacks are going beyond e-commerce, personal or corporate data – the Stuxnet worm confirmed that these attacks now extend to the infrastructure that supports our factories, our energy supply and even our government.

According to the 2010 IBM *X-Force Trend and Risk Report*[7]:

- 2010 marked a year where public and private organisations around the world faced increasingly sophisticated, customised IT security threats.
- 2010 will be most remembered as a year that was marked by some of the most high-profile, targeted attacks that the security industry has ever witnessed.
- 2010 unveiled the evolving, sophisticated face of cyber crime.
- In 2010 IBM documented more than 8,000 new vulnerabilities, a 27 per cent rise from 2009.
- Public exploit releases were also up 21 per cent from 2009 to 2010.

Threats are becoming increasingly complex and the nature of the security threat is changing. For example, responses must now deal with the emergence of advanced persistent threats (APTs), such as the Aurora attacks. These attacks were something of a call to action for the US government, which publicly upbraided China for its alleged involvement.[8]

APTs can be divided into five distinct phases:

1. Reconnaissance.
2. Initial infection.
3. Lateral expansion.
4. Subversion, exfiltration.
5. Clean-up.

While the methods of attack being used in phase 2 are still being built on known concepts, there is much more sophistication being seen in phases 3 and 4. Whereas attacks used to be fairly random and opportunistic, today's attacks may persist undetected, slowly gaining control of critical assets and following a clear plan.

Knowing the risks helps to balance the various defence methods available:

Technical mitigation: firewalls, security patches, network intrusion prevention.	VS	**Non-technical mitigation:** leadership, education, policies.
Financial investment: the cost incurred for effective technical and non-technical threat mitigation.	VS	**Degree of protection:** the level of residual risk that an organisation is willing to accept.
Pre-emptive protection: defensive measures to prevent an incident from occurring. The medieval castle analogy is to build higher and thicker walls.	VS	**Reaction to incident:** the ability to minimise the impact to the business after an attack by responding quickly and bringing the system back to normal operation again.

Cyber attacks

Hacking: breaking into a computer or network to gain some form of control. Techniques include SQL injection, denial of service, access via default credentials, and password or credential theft.

Malware: software designed to infiltrate or damage a computer system without the owner's knowledge or consent – eg, key logging and spyware, malware to establish a botnet, Trojan.

Misuse: abuse of computer systems, abuse of personal privileges for malicious intent, abuse of system privileges, embezzlement.

Deception and social: manipulating an individual to gain unauthorised access to a computer system or network – eg, phishing, pharming.

Physical: trespass or threat to gain unauthorised access to a computer system or network – eg, wire tapping, shoulder surfing, assault/threat of harm.

Combating such attacks requires investment, training and testing in similar environments, as well as remaining vigilant– not every attack will be detected in phase 1 or 2. This means that you must assume that an attack has already succeeded and is slowly taking over the control of critical assets. This requires monitoring the internal network on a continuous basis as well as the perimeter.

As a consequence, security monitoring becomes more challenging because more data has to be analysed and many attacks can be detected only based on the deviation from normal behaviour. In other words, the attack may be detected only once it has progressed for some time.

While the natural tendency of an organisation may be to focus on the technical aspects of cyber security, this will not be sufficient in isolation. The IT infrastructure is as vulnerable as its weakest link. This can be a badly maintained end device, but it can also be an employee who ignores simple security guidelines. Therefore, cyber security starts with an in-depth risk assessment.

There is usually a network of players involved in any attack – an intentional infection is made by one party and its capability is sold on to others to exploit, like a supply chain network. There are multiple parties and motives involved in an attack network. It is much more complex than any effort by an individual.

27%

rise in cyber security vulnerabilities – identified by IBM between 2009 and 2010

THE IMPACT ON THE PUBLIC SECTOR

Confidence in the availability of secure services includes everything from power to drinking water and public infrastructure, all of which are critical to sustaining our everyday life and economic well-being.

As US secretary of state Hillary Clinton stated in 2010, following the Aurora attacks: "The ability to operate with confidence in cyberspace is critical in a modern society and economy".[9] One of the UK government's objectives is to make the UK attractive for companies to do business supported by a national infrastructure that is resilient against cyber threats.

The UK government seeks to create a trusted and safe environment for online services in order to maintain its position as a leading economy with effective e-enabled government services: self-service, citizen-centric and online. This is not solely a government problem – it's a problem for the UK as a whole. Anything that threatens that environment must be dealt with quickly and efficiently.

What does this mean for public sector organisations trying to secure their systems and data against cyber threats? It means the game is changing. Attacks are becoming more sophisticated and more targeted, and they are not limited to public sector departments. They extend to the supply chain that keeps the public sector in business – utilities, telecoms, banks – and the critical national infrastructure supporting that supply chain.

It is this highly interconnected nature of our modern "systems of systems" that requires an ongoing risk-based approach – balancing technical with non-technical threat mitigation methods, where success will be judged by the ability of an organisation to continue with its critical functions and business operations despite hostile activities.

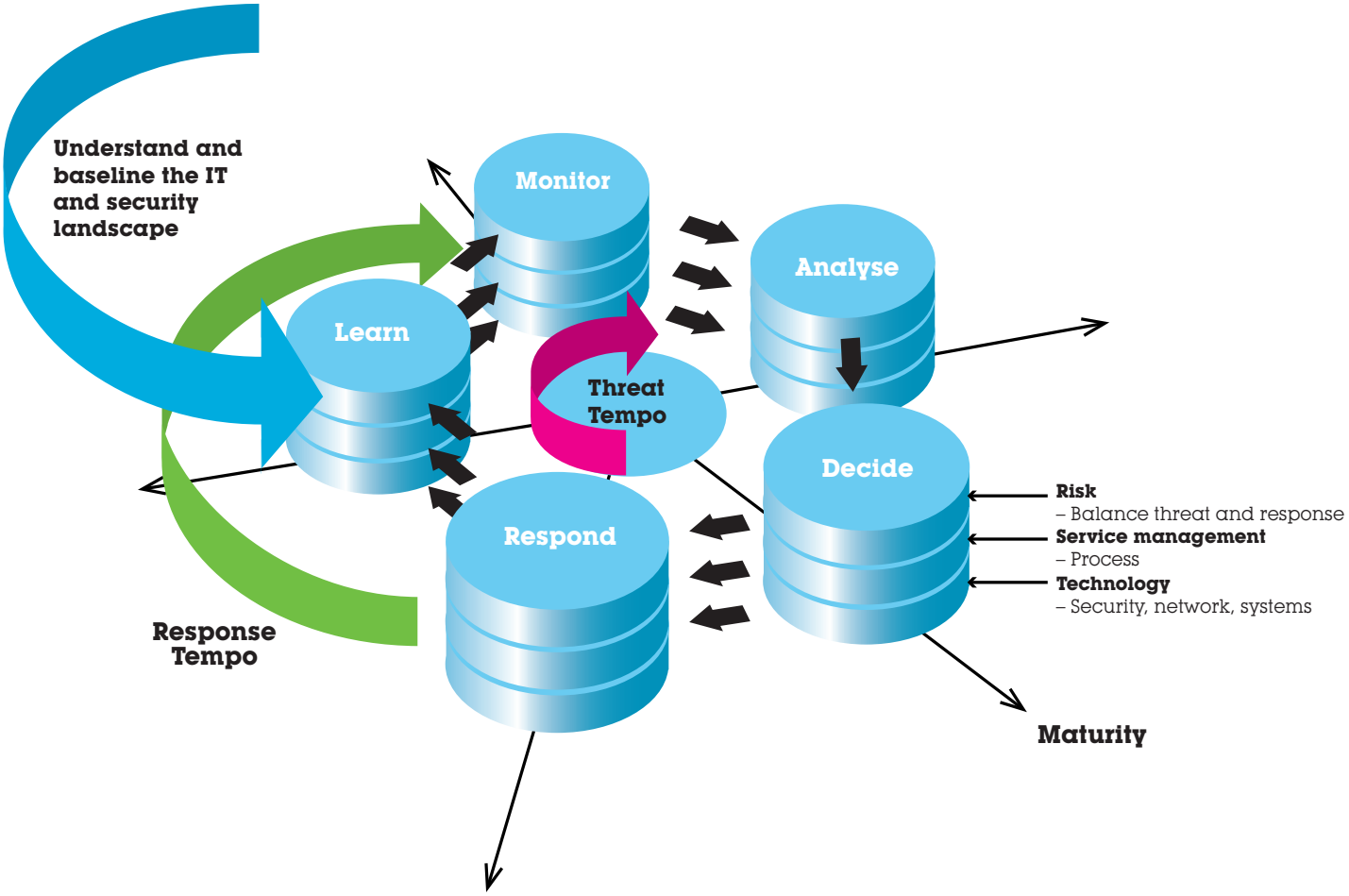
From smart meters on the energy grid to building control sensors, from the pervasiveness of smart phones to devices on open networks using standard protocols, our systems are becoming increasingly instrumented and interconnected – and they are generating large volumes of data in real time. While this may mean increased intelligence for organisations, it also opens the door to more threats and places greater dependency on components in the infrastructure.

A walled garden approach is no longer sufficient. Systems that are linked to the internet are exposed to security threats. The key for organisations is to focus on resilience at the business process level while driving a balanced approach to investment in IT security.

Look at healthcare. In the past, medical equipment stood alone but these days, while one end may be connected to a patient, monitoring or even keeping the individual alive, the other end of the system is commonly connected to an IP network.

There is an inherent risk in data aggregation enabled by interconnectivity. Meaning can be derived by combining lots of innocuous fragments of information, so there is a need to consider not only the types of information being collected but how they are being collected and how the newly gained insight needs to be protected.

The Cyber Security Lifecycle



The public sector is starting to acknowledge the scale of the cyber security problem – the government's National Security Strategy[10] ranks cyber attack alongside terrorism, chemical, nuclear or biological attacks, and large-scale accidents or natural hazards, in terms of the potential damage it could cause.

Ultimately, however, the task and responsibility for overall national cyber security is shared among stakeholders. This implies a huge co-ordination effort, one that will stretch also the non-technical mitigation approaches of policy, training and collaboration to the limit.

For people using public services, education and advice on the basics of cyber security will go a long way to keeping them safe. For those providing the services, however, the threat is very different.

A successful approach to cyber security establishes a risk posture, which then drives risk management and awareness through an organisation or supply chain. Not one size fits all. The question is: what is business critical and what is not; what investment should be made in each area to satisfy that risk appetite?

The threats we face vary with time as well as the national threat level[10] for a potential terrorist attack– for example, as it changes from "Moderate" to "Substantial" and the possibility of a terrorist attack increases. And criticality will vary as operational circumstances change in commercial organisations and well as in government.

THE CYBER SECURITY LIFECYCLE

The tempo of cyber attacks is growing and the speed of the response must keep pace. A lifecycle model can help commercial and public sector organisations to deal with specific situations where tempo, automation and advanced analytics are important, so they are able to detect and respond faster. The key points in the Cyber Security Lifecycle are as follows – though it is important to remember that organisations can enter the cycle at any point. It depends on the maturity of the organisation's security capability and the risks that need to be managed.

LEARN: Understand the IT landscape, including the network topology and the potential risks to the organisation, and detect the vulnerabilities in the organisation's IT infrastructure.
MONITOR: Capture and correlate events from network devices and other IT infrastructure to provide a real-time view of what is happening. Detect that an intrusion has occurred, or that a program or information has been manipulated.
ANALYSE: Understand the nature and significance of an event. Establish the bounds of an attack and visualise the results of this analysis.
DECIDE: Determine how to deal with the incident, balanced against the business impact.
RESPOND: Act. Contain and fix the damage. Determine if and how the attack was successful. Implement deterrents to threats and eliminate known vulnerabilities.
LEARN (the cycle begins again): Using analysis and insight from actions taken, improve the management of risk and predictive analytics. Inform others about the attack and associated preventive measures that should be taken.

In each stage of the lifecycle there are three layers that need to be considered. In addressing the cyber threat it is not sufficient to focus simply on technology, but it is a combination of technology, service management and risk.

For example, if an organisation is under cyber attack and decides that the appropriate action is to change a network configuration, then this decision cannot be made in isolation. The organisation needs to consider the impact of this change from a service management perspective.

Look at change and configuration management, what business services might be affected by this network configuration change; what are the business risks of this change and service disruption versus those of another approach? Technology, service management and risk must be balanced.

These three layers fit into an overall strategy to tackle cyber security and protect an organisation's assets and processes. A security approach that focuses on a single layer will fail. This lifecycle can be used to gauge where your organisation is in terms of cyber threat capability. It requires a faster response, integration and automation of security (including network and systems), real-time service and risk management and integration and automation of the decision loop. Moreover, with the rapidly evolving and expanding nature of threats, organisations need to act now and begin to implement the lifecycle.

LEARN

Understand where you are today.

Organisations with a low level of maturity in cyber security capability would do well to start the process by improving their knowledge and understanding of their assets and defences at the service management layer.

This involves activities such as:

- Identifying, classifying and cataloguing IT and business assets.
- Outlining a organisation's network, system and application topology.
- Understanding vulnerabilities in the network, systems as well as business applications.
- Understanding security awareness and the behaviour of employees and their associated working practices.

IBM can help with all these activities. For example, IBM supports organisations in detecting and assessing IT vulnerabilities, via regular penetration testing and other means. It can help organisations to keep track of how often they are under attack, or how quickly they recover from incidents.

In the risk layer it is key to establish a governance, risk and compliance (GRC) regime at the outset, one that balances cyber security and response strategies with the current assessment of IT and business risks.

Risks in business typically focus on finances, compliance and regulation, but, by creating a GRC regime, organisations put emphasis on those cyber risks that are relevant to them. This can be a separate view of risk from the normal legal, regulatory and contractual views.

The challenge is to measure and manage business risk in conjunction with the technology used to defend the organisation from cyber threats. IBM can help organisations to build a picture by selecting appropriate risk metrics to measure the strength of their defences and help them to understand the risks and threats they face.

A privately owned UK utility company engaged IBM to help conduct a risk assessment of connecting components in process control networks which have traditionally been separate from its mainstream IT estate. Such networks have traditionally used proprietary network protocols such as SCADA.

Security was assured through the physical isolation of the network components and the physical security surrounding the actual devices connected to that network. As we move towards the smart grid, so SCADA has evolved to use the mainstream IP transport.

A prerequisite for defending against cyber threats is to have a clear inventory of the components you need to defend, allied to an accurate picture of the routes through which those components might be attacked. IBM assisted the utility company through a programme of electronic and physical penetration tests, aimed at discovering all possible attack routes to these networks. The results were added to those of a conventional risk assessment to provide a comprehensive risk treatment plan.

9%

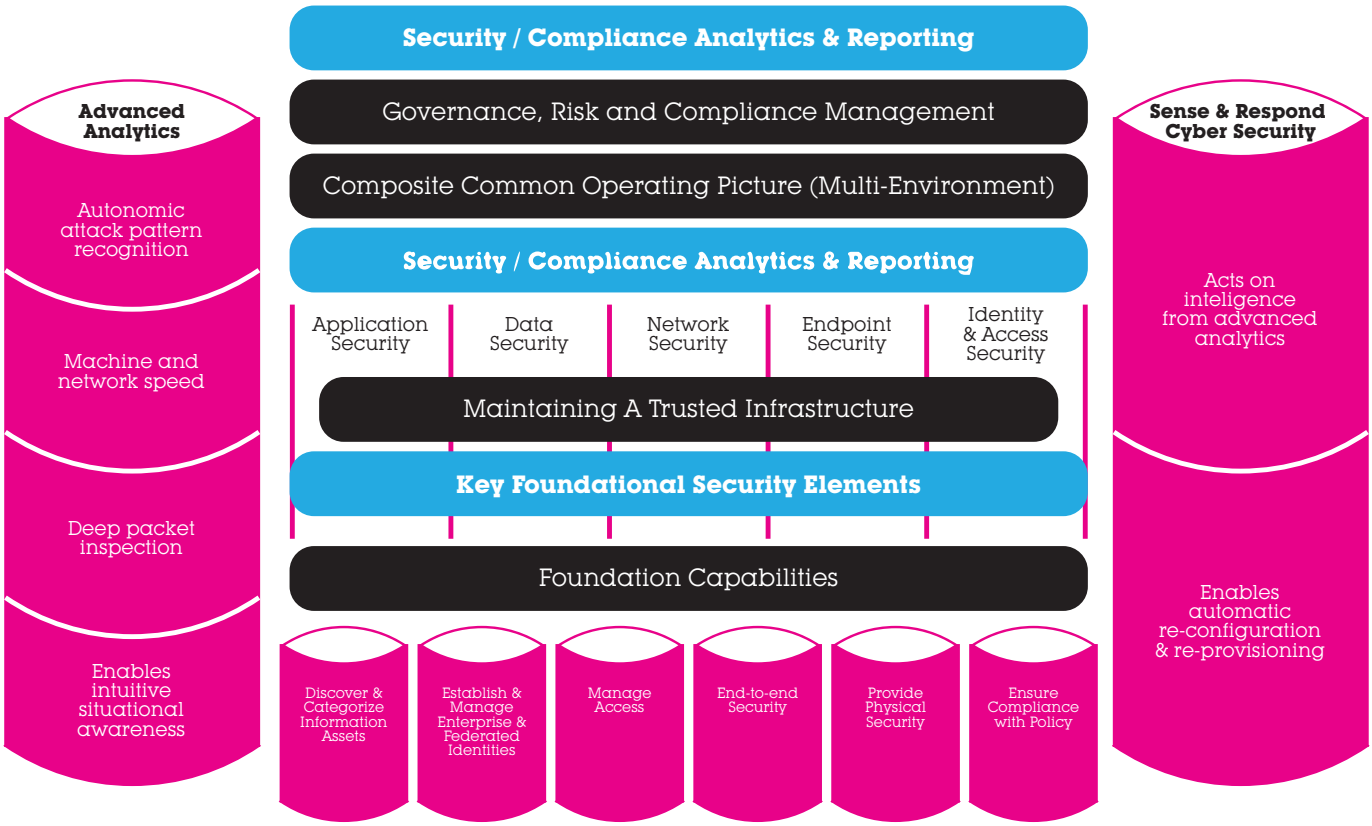
of businesses report a significant attempt to hack into their network in 2010-11[11]

MONITOR

Understand what is happening on the network and IT infrastructure in real time.

Organisations with a solid foundation of protecting the network from both external and internal network attacks will need to continue this approach –

Dynamic Cyber Security: the big picture



but this cannot be expected to be infallible because the nature of threats is evolving. Therefore, protection mechanisms have to be complemented with a comprehensive monitoring strategy that aims to detect suspicious activities.

Robust network architecture designed and built with security in mind from the outset ("Secure by Design") will both help withstand attacks, as well as providing a scalable and effective monitoring platform.

Monitoring is an important line of defence against attacks. Ongoing monitoring will detect known attack patterns but also suspicious activities that deviate from normal behaviour. This can include unusually heavy traffic flow between machines or business applications revealing transactions patterns never seen before.

An effective monitoring system will:

- gather relevant data in real time;
- scan web content for malware and block it before it reaches your organisation, improving your uptime, productivity and business performance;
- audit and alert on privileged user activity for insider threat;
- capture activity that merits further analysis and investigation;
- monitor the network and identify potential exposures;
- gather information to help inform other phases, such as optimisation of the network architecture needed for secure networks.

Visibility of security information improves risk management, allowing incidents to be recognised and handled more quickly, policies enforced and compliance monitored.

For example, over 15 million people (generating more than 450 million page views) accessed the IBM-hosted website for the 2011 Wimbledon Tennis Championships, many keeping track of match progress via IBM's PointStream scoreboard. The web hosting service was provisioned on IBM's private cloud and, as part of its security, IBM deployed its ISS Intrusion Prevention System. This inspects network packets to determine which are suitable to be allowed through to the firewall and helped IBM to stay ahead of threats, preventing up

to 80,000 "attacks" on peak days during the Wimbledon fortnight. Protective monitoring was active in the data centres run by IBM and the sources and type of current attacks were displayed on a global threat map.

ANALYSE

Understand the nature and significance of an event. Establish the bounds of an attack. Visualise the results of this analysis.

In the public sector, new capability is essential in order to analyse cyber threats in real time and predict threats. The traditional security approach is important but not sufficient to tackle today's cyber security challenges – the speed, volume and variety involved are substantial. Today's cyber threats require:

Continual inspection and analysis of high volumes of dynamic data from sensors and other devices to gain accurate insights into possible threats and system compromise in real time. Pattern and behavioural analysis across diverse data streams from many channels is necessary to detect evasive attacks. Organisations need to be able to execute complex streaming analytic systems capable of extracting deep insight from huge volumes of data in milliseconds instead of minutes or hours. The threat appears at increasing speed and deep analysis is critical to defence within that same time horizon. Cyber is ultimately a big data problem.

Advanced situational awareness provides the context and alerting to enable decision making (next step of the lifecycle) and appropriate response in circumstances when humans cannot keep up with the pace of the threat when under attack. Your defences need to be able to fuse information from a variety of sources, including real-time observations, and make them available within the right context. This analysis will have an impact on business processes that will need to be thought through carefully and automated in order to adapt and respond to the threat dynamically.

Learning new patterns from historical analysis for predictive capability.

80k

cyber attacks per day on Wimbledon's website are thwarted using IBM cyber security

Ultimately, effective analysis is based on a very simple idea: knowing what happened and why is good, but being equipped to act while events are unfolding is better. In order to achieve this goal, there are some essential tools that will play key roles in the Analysis phase of your Cyber Security Lifecycle.

Using these analytical tools, organisations will be able to maintain constant assessment of the threats they face and respond accordingly. For example, the US Federal Aviation Administration (FAA) is working with IBM on a project to protect the nation's civilian aviation system from cyber attacks. The scalable prototype security system will introduce analytics to protect large digital and physical infrastructures from hacking, botnets, malware and other cyber attacks.

The system will review event occurrences and system compromises. It will correlate traffic patterns with dynamic data from monitors, sensors and other devices capturing information about network traffic and user activity in real time.

Streaming analytics will be a key design component of the FAA prototype system, covering the massive amounts of data flowing through its networks in real time, producing insights into possible threats and system compromises in time to take action. The FAA will also be able to store the results in a data warehouse for analysis and supervised learning.

DECIDE

Assess the attack to determine how to deal with it.

First and foremost, effective decision models stem from the risk posture taken by the organisation, based on the understanding of the IT landscape gathered in the Learn phase. In other words: you need to know what you are going to do and why, based on the assets you know you want to protect and the risks they face.

Second, it is critical that decision-making processes be carefully thought through and automated to adapt and respond to the threat dynamically. The decision-making process involved in cyber security should not depend entirely on human intervention – when under attack, humans cannot keep up with the pace of the threat. Where human involvement is required, analytics must distil pertinent information to present to decision-makers, who in turn must be available and empowered to decide what action to take. Advanced analytical systems should be linked to service management throughout the network, with automated decisions in place regarding specified threats to the infrastructure or other detailed criteria. While there is the risk that false positives will trigger some unintended responses, this needs to be weighed against the value of continued service and the amount of harm that could be caused by an attack.

Thinking of all the scenarios in advance is difficult, but a degree of preparation is possible – such as by making good use of workflow capabilities in service management tools.

For example, the US Air Force is working with IBM on a secure cloud computing infrastructure capable of supporting defence and intelligence networks, using advanced cyber security and analytics technologies in the cloud architecture. The infrastructure design will support large-scale networks and meets the government's information assurance guidelines for all networks.

Customised executive-level dashboards will deliver real-time information on the health and status of the network and facilitate decision-making. Advanced stream computing analytics will be used to analyse the data flow and produce fast, accurate and actionable insights about possible threats.

This instant access to information would, among other things, enable officials to shift the prevention environment automatically based on rules-based protocols in the event of a cyber attack or network anomalies.

Autonomic computing will enable virtual cloud services to be managed remotely and provide capability for the cloud infrastructure to retune itself constantly for optimal performance – without human intervention.

RESPOND

Contain and fix the damage.

Some attacks are going to get through – that is the evolving nature of cyber security. The key is how you respond. You need to determine how the attack was successful and respond accordingly, implementing measures to deter further threats. Reduce known vulnerabilities in the network and business applications, then set up and reconfigure the network to withstand another similar attack.

Ideally, you will have automated your business processes to adapt and respond to the threat dynamically – it is a question of dynamic management of the infrastructure. Many organisations want to be able to respond by pulling big levers – a "kill switch" of sorts. This requires up-front design of operational and business support systems. Depending on the threat, it may be just as effective to quarantine a network, detach virtual machines or remove an infected workstation from the network.

Using deep analysis to perceive conditions, including insider threats, defence strategies can be established that execute via pre-authorised autonomic reactions at machine speed. This can go as far as reconfiguring network connections and shutting off network ports as needed. Systems should be able to expand the virtual resources dedicated to an application as well as changing security policies.

Most important, learn from the attack. Using analysis and insight from actions taken, improve the management of risk and predictive analytics. Inform others about the attack and associated preventive measures that should be taken. And so the cycle begins again.

IBM is deploying its Tivoli Endpoint Manager, built on BigFix technology, internally to transform its workstation and mobile security infrastructure. In response to the ongoing challenges posed to protecting endpoints, infrastructure and data by the ever-increasing volume and frequency of security threats and attacks, IBM has demonstrated in a pilot that it can improve patch availability and achieve 98 per cent success in patching endpoints within 24 hours. With 425,000 employees, IBM is moving from a model of user reliance to automation for remediation where specific actions target an exact type of endpoint configuration or user type. Like other organisations, IBM evaluated the business value of extending the Tivoli Endpoint Manager pilot to all of IBM's endpoints. IBM has estimated it can reduce workstation security issues by 50 per cent within the first year, an estimated $10 million in cost savings.

IBM has begun a worldwide internal deployment of Tivoli Endpoint Manager. At the time that this document was published, IBM had deployed Tivoli Endpoint Manager to over 550,000 endpoints within six months, out of a total of 750,000 Windows, Mac and Linux endpoints targeted by the end of 2011. Expansion to include mobile endpoint management (when available) is also planned.

IBM Tivoli Endpoint Manager combines endpoint lifecycle and security management into a single solution that provides visibility into physical and virtual endpoints. By automating time-consuming tasks across complex networks, organisations can reduce risk by maintaining compliance with internal security policies, and respond more quickly and effectively when they discovery a cyber threat.

50%

reduction in workstation security issues can be achieved within the first year

WHY IBM?

IBM has a record of helping organisations to achieve effective cyber security. IBM manages end-to-end security for customers across the world – not only the technology involved, but the human element as well. IBM Security Solutions provide a holistic approach, which can allow organisations to securely, safely and confidently adopt new technologies.

Our success in the design and delivery of secure systems to government is achieved by working alongside government accreditors, security advisers and CESG to ensure security requirements are considered in the design, reviewed during development and checked for compliance during testing to gain assurance and accreditation. Using established certified products, reusing the configuration of hardened assets and undertaking rigorous code reviews by both developers and security specialists, IBM helps clients build and operate systems that are secure by design.

IBM employs its X-Force research and development team to provide a clear and current picture of cyber threats and attacks. It has global reach and understands the threats in detail. IBM has nine Security Operations Centres and nine Security Research Centres globally. The information from these teams enable us to understand and remediate threats and help organisations harnessing the thousands of researchers, developers, consultants and specialists focused on security worldwide. Information and intelligence from this research and the day-to-day operational view is constantly fed back into IBM Security Solutions. Monitoring security devices worldwide for thousands of clients across 133 countries, 13 billion events per day gives IBM the information about new threats and attacks first hand. IBM recently launched the IBM Institute for Advanced Security to further strengthen these efforts and bring these capabilities together across the company to help organisations tackle these cyber security challenges.

Cyber security is about managing a spectrum of risk. Focusing on desired business outcomes, organisations can take a balanced approach to protecting their assets by weighing up risks against the costs of mitigating them. Some attacks may get in; the question is how you manage and limit their impact. IBM understands the pace and scale of threat that customers may face and provides the technology and support needed to make decisions. IBM offers advanced security analytics and its integration with service automation, helping businesses to assess the impact in order to make decisions and deal with the threat.

There are building blocks that are essential to increasing maturity using the cyber security lifecycle in any organisation. The following five entry points provide some examples.

1. UNDERSTAND MY BUSINESS ASSETS

"How can I get a clearer view of my organisation's critical business assets and create a register of possible cyber risks faced by those assets, so I can manage them better?"

Cyber Security Lifecycle entry point: Learn

IBM has a variety of offerings to analyse, assess and record the risks, so that the organisation knows what it has, understands the risks to its assets can prioritise and target investment to protect them. These range from:

1. A two-day cyber security workshop that highlights the range of threats and their potential impact and identifies key business and IT assets that are vulnerable and illustrates possible mitigations; to
2. A more in-depth assessment of an organisation's current security environment relative to business requirements and goals regarding information security.

2. UNDERSTAND MY IT ASSETS

"How can I get a clear picture of which infrastructure components are being used to deliver business services so that I can see any dependencies that may exist when dealing with threats and attacks?"

Cyber Security Lifecycle entry point: Learn

A clear view of the components supporting particular business services is a key prerequisite to enabling an effective response in the face of a cyber threat or attack. IBM is able to automatically discover individual IT assets, their configuration and the interdependencies among them.

A comprehensive repository of this information can be used to understand the link between components and business services and business applications. Currency of information is maintained allowing vulnerabilities arising from incorrect or out of date configuration to be addressed.

This insight informs the decision making process with accurate, reliable information. Any action taken in response to a situation can then be viewed with confidence.

3. PROTECT MY IT ASSETS

"How do I ensure a base level of protection for my IT assets from both outsider threats and insiders?"

Cyber Security Lifecycle entry point: Respond

Identity and access management is a cornerstone of good IT asset protection. In particular the management of privileged user access rights requires careful planning. As needed, identity and access management can be complemented with data security mechanisms such as the encryption of sensitive data including the proper key management. Network security capabilities, such as firewalls, intrusion prevention systems, or data leakage prevention systems add another layer of defence.

Asset usage can be monitored and analysed – both at the host and at network level – to detect suspicious activity. Monitoring asset usage is not only relevant from an asset protection perspective; it can also be required for audit and compliance purposes.

Given its broad range of security products and services, IBM can assist customers in all these tasks, from their initial implementation to their ongoing operation.

4. USERS!

"How can I improve employee behaviour and awareness, and increase the security of their access points?"

Cyber Security Lifecycle entry point: Respond

IBM offers education for employees to raise their awareness of the potential threats to encourage appropriate behaviour.

Alongside this, technology can be applied continuously to achieve compliance of the endpoints they use. Automated data gathering and reporting of endpoint configurations and infrastructure can identify security issues as they occur. Centralised remediation action can be taken, such as to push out and enforce the installation of patches with a high degree of accuracy. Such changes can be deployed in the infrastructure and verified in response to a threat or attack.

This combination of learning and IBM technology ensures that endpoints are properly configured and fully patched, closing most exposures from a user perspective arising from naivety, negligence, phishing, mis-configuration and media handling. Reducing the number of security incidents caused by users lowers operational costs.

5. MANAGE MY IT SECURITY

"How can I manage my IT assets better by applying industry expertise and security operations in a cost-effective fashion?"

Cyber Security Lifecycle entry point: Monitor

A managed security services approach enables organisations to harness expertise, tools and infrastructure needed to secure your information assets from internet attacks, often at a fraction of the cost of in-house security resources. IBM provides a view of your security infrastructure in a single management console. It allows you to mix and match by device type, vendor and service level to meet business needs while accelerating protection, simplifying security management and reducing security costs.

Information captured in the delivery of such a service can be used to provide trend and security intelligence in order to enable increasingly effective protection.

BRINGING IT ALL TOGETHER

The Cyber Security Lifecycle enables continuous assessment and improvement through the application of risk analysis, techniques, best practices and technology.

IBM has a wealth of experience securing systems in both public sector and commercial organisations. By protecting UK national infrastructure we sustain trust and confidence in public services.

THE AUTHORS

Chris Nott
UK Public Sector Technical Leader
IBM Software Group
M: +44 (0)7831 531241
E: chris_nott@uk.ibm.com

Martin Borrett
Director of the IBM Institute for Advanced Security Europe

Dr John Marc Gibbons
UK Public Sector Technology Strategy Leader, IBM Global Business Services

John Palfreyman
Director – Defence & Public Safety, CTO Office, IBM Software Group Europe

Dr Andreas Wespi
CTO Office, IBM Software Group Europe

Acknowledgements

Phillip Jolley
Executive Partner, Defence & Public Safety, IBM Global Business Services

Mark Palmer
IBM Industry Executive, Defence & Public Safety

Dr Graham Spittle CBE
Chief Technology Officer and Vice President, IBM Software Group Europe

IBM Institute for Advanced Security

The IBM Institute for Advanced Security helps organisations to better understand and respond to the security threats to their business. It draws together IBM's understanding and experience of how to secure an organisation's assets using technology by applying the industry's latest insights and best practice. It operates globally, recognising the need for access to local expertise; it has branches for Europe, the Americas and Asia Pacific. Each harnesses IBM Security Research including X-Force and IBM's Security Solutions.

References

1 "Managing Threats in a Dangerous World: The 2011 Business Continuity Management Survey". March 2011. Patrick Woodman and Paul Hutchings. Chartered Management Institute

2 "A new approach to China". 12 January 2010. http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

3 "Malware Aimed at Iran Hit Five Sites, Report Says". New York Times. 11 February 2010. http://www.nytimes.com/2011/02/13/science/13stuxnet.html

4 "I.M.F. Reports Cyberattack Led to 'Very Major Breach'". New York Times. 11 June 2011. David E Sanger, John Markhoff. http://www.nytimes.com/2011/06/12/world/12imf.html

5 "CIA website hacked; LulzSec takes credit (again)". Consumer Reports. Consumers Union. 16 June 2011.

6 IBM X-Force Threat Reports. http://www-935.ibm.com/services/us/iss/xforce/trendreports/

7 IBM X-Force Trend and Risk Reports, op cit

8 "Google hacking allegations 'very serious' says Clinton". The Guardian. 2 June 2011. Esther Addley, Adam Gabbatt, Charles Arthur, Jonathan Watts. http://www.guardian.co.uk/world/2011/jun/02/google-hacking-allegations-serious-clinton

9 "Statement on Google Operations in China". Hillary Rodham Clinton, Secretary of State. US State Department. 12 January 2010. http://www.state.gov/secretary/rm/2010/01/135105.htm

10 "A Strong Britain in an Age of Uncertainty: The National Security Strategy". http://www.direct.gov.uk/en/NI1/Newsroom/DG_191679

11 "Managing Threats in a Dangerous World: The 2011 Business Continuity Management Survey", op cit.

IBM United Kingdom Limited
PO Box 41
North Harbour
Portsmouth
Hampshire
PO6 3AU

The IBM home page can be found on the internet at ibm.com

Produced in the United Kingdom
September 2011

BUW03020

Recycled fibre content: 50% post-consumer waste, 25% pre-consumer waste and 25% virgin fibre.