

Cyber Security

White Paper

Konstantinos Tzannetakos, Activity

The purpose of this white paper is to provide an understanding of the cyber threats organisations are currently facing, the risks posed by those threats and to outline countermeasures for effective mitigation. Although many organisations have increased investment in information assurance and security, only an effective strategy and plan is appropriate to counter current cyber threats.

Table of Contents

Introduction.....	2
Cyber Security Threats.....	2
Types of Cyber Threats	4
Which organisations are at Risk?.....	4
What Action you should take	6
For More Information	8
Biography of Author	8
About Activity.....	8
Glossary	11

Introduction

A decade ago, cyber security was considered a priority, but was mostly a concern for government and military computer networks processing sensitive and/or mission-critical information. These networks were protected to an extent that any unauthorised access should not be feasible or possible from potential adversaries. The impact of a successful intrusion would be devastating, but the numbers of actual incidents were quite few and even fewer would see the light of day.

Nowadays the threat of cyber attack is not only a concern for government and the military. Cyber attacks against commercial organisations also hit the news. All organisations now rely on an online presence, yet the two main components of that presence, Email and web sites, are the two main attack routes which cyber attackers use to compromise corporate networks. Cyber attacks can result in business disruption causing financial damages and impact brand reputation, or the loss of key intellectual property threatening the long-term competitiveness of a business. With the proliferation of free hacking tools, every single organisation is constantly scanned, probed and attacked and is a potential cyber attack victim and the next news story.

Cyber Security Threats

The reported incidents show that cyber attacks are not rare and that attackers have been increasing their activity against a range of both government and private networks.

“Operation Titan Rain” was the name given to a series of persistent cyber attacks which go back to 2003. The attacks were against US government and military networks. Cyber attackers managed to gain unauthorised access to organisations such as Lockheed Martin and NASA resulting in the stealing of industrial secrets and innovative technology. In 2005 Distributed Denial of Service Attacks (DDOS) against Estonia and Georgia were performed originating from Russian hackers as retaliation during the crisis between these nations.

Researchers from the Information Warfare Monitor with the help of the University of Cambridge Computer Laboratory discovered in 2009 a large scale cyber espionage operation against 103 countries. Embassies, ministries and high profile political figures had been targeted. Cyber attackers participating in “Operation GhostNet” used spear phishing to infect and afterwards monitor the activities of their victims.

The list of organisations targeted by cyber attacks includes those in Financial Services, Aerospace and Defence, Energy, Health Care, Construction, Manufacturing, Law Firms, Pharmaceuticals and Biotechnology, Information Technology and Research Industry.

At the start of December 2009 Google announced that it had been targeted by sophisticated, determined, organised cyber attackers. These attackers, or Advanced Persistent Threat (APT) and their infamous “Operation Aurora”, as they are now more commonly known, were dedicated, well-funded professionals whose sole purpose was to gain unauthorised access and steal intellectual property rights from Google. It was also discovered that Google e-mail

Cyber Security

accounts of Chinese human activists had also been compromised. This incident was the key to unveiling the largest cyber attack against a series of organisations, among them were Adobe Systems, Juniper Networks and Yahoo. The APT's sole purpose was to steal knowledge, corporate secrets and innovative technology. In the case of Adobe, the attacks purpose was to gain knowledge of unknown vulnerabilities in the client software such as Adobe Acrobat Reader and Adobe Flash Player. As these programs are used pervasively across all industries and computer systems, their vulnerabilities can be exploited to compromise a wide range of organisations. Adobe PDF exploits and JavaScript obfuscation are particularly popular techniques used to hide malware in innocent-looking document files such as PDFs.

The persistent threat against government and military targets has expanded to strategic targets such as energy supply which were considered primary targets for kinetic attacks in warfare, and now are primary targets of cyber warfare.

The Stuxnet worm which was first seen in the wild in July 2010, revealed how a cyber weapon can infect Industrial Control Systems and SCADA controllers. Security researchers were surprised at the sophistication of this worm. According to anti-virus companies, Stuxnet included many attack vectors. Stuxnet primarily would spread via USB sticks in order to infect computers and networks not currently connected to the Internet. It would exploit systems by delivering a number of both patched and unknown "zero-day" vulnerabilities in the Windows operating systems. In addition it installs its own system driver to the compromised computer, circumventing security controls by using two stolen digital certificates. The target of Stuxnet was a particular model of Programmable Logic Controller (PLC) made by Siemens. SCADA PLCs are small embedded industrial control systems which are responsible for automated processes in a wide range of industrial plants. Stuxnet would use a rootkit specifically designed to remain stealthy. Although the worm infected thousands of Windows systems, it is not responsible for any known physical damage, though it is believed it caused the failure of India's INSAT-4B satellite and infected the Iranian Bushehr nuclear plant. Stuxnet was a sophisticated malware, which required considerable expertise and resources to produce. It is definitely a product of modern cyber warfare.

Cyber Crime is also on the rise. Organised crime is focused on Return on Investment (ROI) and has been quick to establish its presence in cyber space. Worldwide gangs and other criminal organisations are invading the cyber world. Cyber crime has already developed an underground economy of cyber fraud, credit card fraud, phishing etc. Their business model is very successful in stealing and then exploiting sensitive personal information. With the recent economic break down, thousands of computer-savvy techies have teamed with cyber criminals to create their own software development and research houses, finding new ways to steal and expand their profitable market. Zeus is the most popular crime ware toolkit. It is now on version 2.0 and is being sold as the easy to use, out of the box, ready to build botnet. It performs a series of attacks ranging from stealing personal data from computer systems to performing Distributed Denial of Service Attacks (DDOS). Cyber criminals have been using it extensively to perform bank frauds and steal money by harvesting credentials from web forms and collecting bank account information.

Types of Cyber Threats

To summarise there are three major threats against the security of modern organisations:

- **Cyber Warfare attacks:** These attacks are highly organised, with nation state support and resources. Their aim is to selectively target military and critical resources and facilitating kinetic attacks to gain strategic advantage. Another goal could be disruption of services or blacking out a whole region and even pushing political propaganda. Cyber warfare targets vary from government or military to Transportation, Oil, Gas, Utilities, Water as well as Aerospace and Defence. The victims of these attacks can never be limited to military but often the unavailability of critical services has a cost to civilians.
- **Cyber Espionage attacks:** or Advanced Persistent Threat as they are known, are determined, organised, highly determined professionals whose sole purpose is to steal intellectual property or trade secrets by infiltrating corporate networks. Their advanced covert methods make them difficult to detect. Industries which are likely to be targeted by Cyber Espionage include Pharmaceuticals, Government, Aerospace & Defence and Consumer Electronics Industries. Gaining competitive advantage by exploiting the information acquired is their ultimate goal.
- **Cyber Crime:** Although not so coordinated or professional, cyber criminals are driven by financial gain. Sophistication of cyber crime ranges from individuals or groups working with little structure or preparation, to complex organisations with advanced preparation, specific targets and objectives. Organisations in Finance, Government, Healthcare, Insurance, and Telecoms are the prime targets. Phishing scams, spam, credit card fraud, identity theft, computer intrusions, child pornography, international money laundering, are amongst the growing list of cyber crimes.

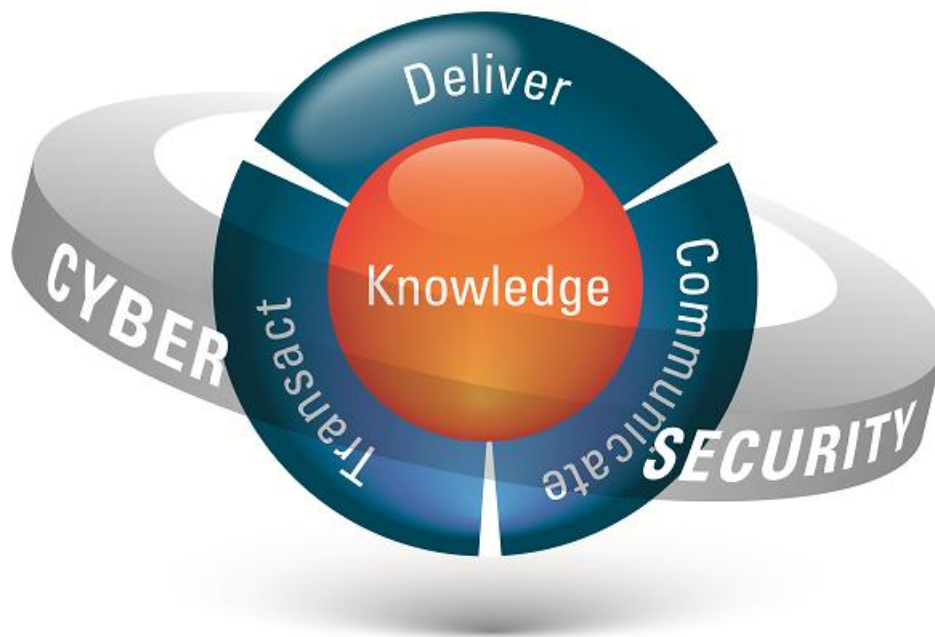
Which organisations are at Risk?

The most threatening cyber attacks would be ones that could disable critical infrastructures: causing power outages, disrupting transport, or disabling key industrial plants. These attacks could deprive large populations of essential services for extended periods of time causing widespread disruption, adverse economic impact and potentially aiding conventional attacks. Critical National Infrastructure providers are threatened by these attacks.

Nowadays, the majority of organisations heavily rely on the Internet and regularly handle valuable confidential and proprietary data. They use it daily for internal and external communications, research, customers, service requests and online purchases. Online connection and presence is important and the majority of the modern world is dependent on it for day to day operations. What kind of data is considered sensitive? Customer data, financial records, credit card information, private information, employee personal data and intellectual property are all valuable assets which need to be protected. Moreover, critical infrastructure, nuclear and power plants, the whole economy of the modern world relies on

Cyber Security

the Internet. Unfortunately, cyber space is built on an insecure platform and is a rich environment for a series of adversaries to plan, hide and execute effective cyber attacks. Modern businesses are potential targets and often easy victims for cyber criminals.



All organisations rely on their corporate knowledge for their survival. This encompasses both intellectual property and business processes that give them their competitive edge. In order to engage with clients and suppliers electronically, companies need to be able to deliver, transact and communicate in cyber space whilst protecting their corporate knowledge and maintaining the availability of their infrastructure. Cyber security protects an organisation against attack on its intellectual property and business processes.

One of the biggest cyber threats is the theft of business information. The amount of value a business can create is often dependent on maintaining the confidentiality of its intellectual property. The theft of such information can eliminate this competitive advantage. A cyber attack focused on information theft could potentially cause businesses or even entire national industries to lose their competitive edge in the global economy.

It has to be emphasised, that the most important and valuable asset of an organisation is the knowledge held within the people, the processes and the operation of the business. Cyber attackers have realised this and have started to break away from traditional opportunistic attacks to focus on targeting individual victims. In the past, attackers were more opportunity-focused, launching attacks blindly on targets that suffered from a specific vulnerability. Choosing their victims and then constructing an attack based on their victims' environment is their new strategy. When attackers start to move away from traditional methods and begin to focus their attacks, whom will they target? Obvious targets are the executives of large corporations, this would include Chief Executive Officers (CEOs), Chief Financial Officers (CFOs), and Chief Operating Officers (COOs). These highly placed individuals in an organisation probably have access to information on their laptops of high value to a competitor.

Cyber Security

Information regarding knowledge, intellectual property, corporate goals and agendas, emails to and from board members, or even data relating to potential acquisitions is extremely valuable. Once the cyber criminal has collected this information, the next step is to convert it to currency. A cyber criminal accomplishes this by selling the information to a competing organisation, selling the information back to the company he stole it from, or investing in companies that the targeted organisation will acquire. Obviously a company's intellectual property is of value to many parties other than the originating company. The information acquired can consequently be used to accomplish goals like gaining competitive or economic advantage by stealing trade secrets and cloning innovative technology.

What Action you should take

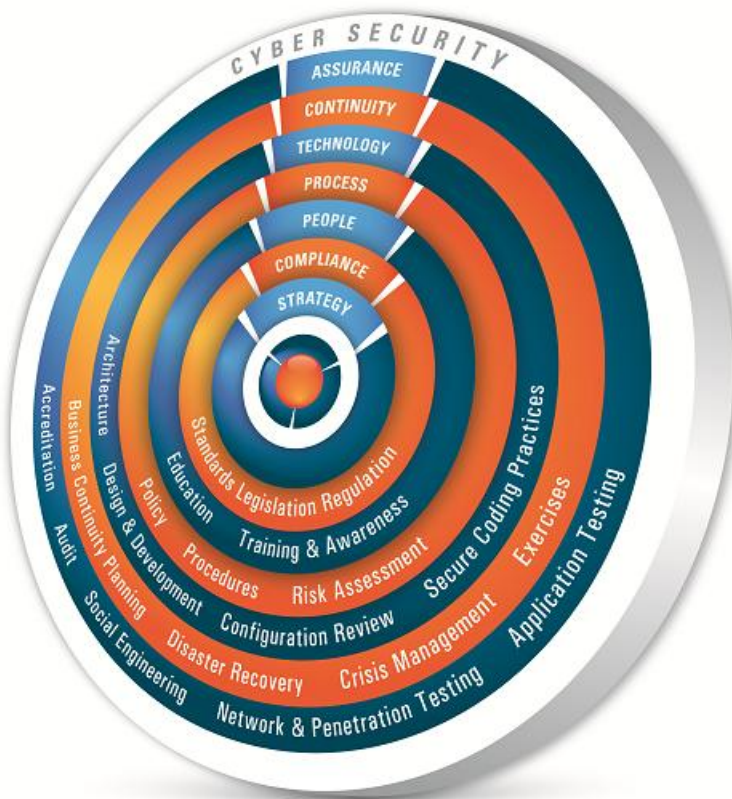
Without a proper cyber security program and regular assessments from security experts how can businesses be assured they are safe from hackers, malware and cyber attacks? Lacking the internal resources, formal policies, employee training and with the latest computer attacks, what would a response be after a compromise from cyber attackers?

The solution or methods to counter these threats exist and are nothing new. By developing a robust information assurance program, an organisation can effectively manage and protect their valuable assets as well as mitigate the risk by:

- Establishing an Information Security Management System (e.g. ISO 27001) which will ensure that security is managed well and the right processes and procedures are in place and available for proper incident handling.
- Performing security risk assessments so that critical business processes, including the technology that supports them (servers, databases, applications) are identified and prioritized, so that the key threats to the organisation are established.
- Performing business continuity planning and disaster recovery to continue operations in the event of a worst case scenario which can disrupt the business.
- Investing in security awareness training. The weakest link in security is often employees doing the wrong things, such as visiting a malicious website or opening an attachment, risking the overall security of an organisation. Educating employees on the latest cyber threats, informing them what they can do to help protect critical information assets and how to report fraudulent or suspicious activity. Verifying that the security awareness training invested by your organisation is understood by the employees and properly assessed by performing social engineering and open source Intelligence tests.
- Deploying technical security measures according to your risk assessment. Security in depth is the best practice, by adding several layers of security as well as monitoring to help identify the severity of a security event. Critical business data should be encrypted, and logging should be performed of all changes to maintain an accurate audit trail. Secure mobile devices when travelling and contact technical support to perform remote deactivation in case of items being lost or stolen.

Cyber Security

- Verifying that the technical security measures are effective and properly configured. Perform regular network penetration testing and application testing against commercial off the shelf and bespoke applications to assess the security of your infrastructure.
- Security of integrated Enterprise Resource Planning (ERP) is paramount. ERP security is not just about bits and bytes but about business transactions which can be abused from system based fraud and errors, inflicting financial losses. ERP vendors want to provide more value to their customers by adding new functionality but unfortunately security often comes as an afterthought. The ERP system has to be properly configured, monitored and secured.



For More Information

For more information contact:

Activity Information Management
25 Hercules Way
Aeropark
Farnborough
Hampshire
GU14 6UU
Tel 01252 377321
Fax 01252 377670
Email info@activityim.com
Web www.activityim.com

Biography of Author

Konstantinos Tzannetakos is a Security Consultant at Activity with an extensive background in IT and Security technology. Prior to working in the UK Security Industry, Konstantinos was performing vulnerability assessments and network administration for military and private networks. He also worked as a researcher at the University of Athens. A paper developed as a result of his research was presented at a worldwide IEEE conference. His current research interests are in the field of network penetration testing, intrusion detection and prevention.

Konstantinos qualifications include a BSc in Computer Science and Communications from University of Athens and an MSc in Information Security from Royal Holloway University of London. He is a member of IEEE, a GIAC Advisory Board Member, and is a GIAC Certified Penetration Tester (GPEN).

About Activity

Established in 2004, Activity is an independent specialist information security consultancy that helps commercial and public sector organisations protect their data networks, business information and online assets. Activity provides advice on best practice information security and business continuity strategies to a wide range of organisations from mid-sized companies to world leading enterprises, government institutions and public sector services. Activity's clients include the Ministry of Defence, Cabinet Office, Metropolitan Police Service, Atos Origin UK.

Accreditations

Activity is a member of the Council of Registered Ethical Security Testers (CREST) and the CESG CHECK Scheme. Many of its consultants are members of the CESG CLAS scheme for security consultancy advice and are PRINCE2 qualified. All of Activity's services are independently certified to comply with the international standards for quality (ISO 9001) and information security management (ISO 27001).

Cyber Security

Services

Information Security Consultancy

Assignments delivered by Activity include the development of security architectures; advice on the requirements for connection to the Government Secure Intranet (GSI); security risk and analysis and the development of security policies (including HMG-compliant policies).

Business Continuity Management

Activity provides independent advice on crisis management, business continuity management and disaster recovery. Activity's business continuity services are BS 25999 compliant and include business continuity document review and audit, business impact and analysis, the development of business continuity strategies, business continuity planning and testing, disaster recovery planning and testing.

ISO 27001

Activity provides advice on ISO 27001 compliance, the international standard for Information Security Management Systems implementation, and enables organisations to achieve compliance with or certification against this standard. Activity helped Atos Origin UK gain ISO 27001 compliance in 2006, one of the largest companies to gain certification against the new international standard.

Information System Audit

Activity provides a comprehensive service to review security risks, procedures and system implementation against legislative, regulatory and business requirements, to confirm that controls are effective and appropriate. This service covers all aspects of an IS Audit including:

- IT Governance & Compliance
- Risk Assessment
- IT Controls
- Business Continuity & Disaster Recovery
- Physical Environment
- Personnel and HR Procedures

Security Testing

Activity provide a full range of security testing services that assess the technical threats to an organisation's networks and applications, from Network Penetration Tests and Host Configuration Assessments to Web Application Security Assessments, full Enterprise Application Security Reviews, Wireless Security assessments and Social Engineering. Activity's structured and repeatable methodologies build on those provided by the CESA CHECK Scheme, OSSTM and OWASP.

Cyber Security

Enterprise Solutions Assurance

Activity provides clients with in depth, independent and balanced advice on the security of their Enterprise Solutions. Enterprise Solutions contain key information on a client's products, staff, customers and suppliers. It needs to be defended from leakage, loss or modification in the same manner as all key information assets. Due to the size and complexity of Enterprise Solutions, technical security is not always addressed at all levels.

Our experienced security consultants have the expertise and specialised tools to conduct non intrusive yet very comprehensive security assessments of your Enterprise Solutions environment.

End-to-End Security Review

Activity deliver a technical security auditing programme that covers all aspects of the security enforcing components of an application encompassing physical, technical and procedural perspectives. The review may include an assessment of security design specifications, system documentation, implementation strategies, integration and operational management. It typically includes a combination of documentation reviews, interviews with key stakeholders, configuration reviews and a proactive technical assessment and analysis of the system itself.

Glossary

APT	Advanced Persistent Threat
ERP	Enterprise Resource Planning
DDOS	Distributed Denial of Service
ROI	Return On Investment
SCADA	Supervisory Control and Data Acquisition