Current and Emerging Threats to Information Technology Systems and Critical Infrastructures

a report by

Matthew G Devost

President, Terrorism Research Center, Inc.

Matthew G Devost is President of the Terrorism Research Center, Inc., overseeing all research, analysis, assessment and training programmes and also providing strategic consulting services to select international corporations and governments. Mr Devost has been researching the impact of information technology on national security since 1993 and is an award-winning author and international speaker on the topics of cyberterrorism, critical infrastructure protection and information warfare.

A vital component of a proactive security posture is an analysis and understanding of the threats facing an organisation. Unfortunately, the dialogue regarding information technology (IT) threats is riddled with invocations of security clearance requirements, soundbite rhetoric and the lack of common threat categorisation. As a result, the private sector is expected to make risk management decisions in the absence of a valid threat context. Threat assessments must be conducted to complement vulnerability assessments and enable organisations to make educated decisions to guide their security programmes and spending. The purpose of this article is to provoke discussion regarding potential threats in the hope that more organisations will take the initiative of investigating the realistic threats facing IT infrastructures.

In response to a frequently voiced concern, the threat of a large-scale critical infrastructure attack in today's environment can be characterised as follows:

- those with the intent lack the capability;
- those with the capability lack the intent; and
- both of the above are subject to change.

To make responsible risk management decisions, it is important to avoid overreaction and also important not to systematically disregard the full spectrum of threats for lack of empirical evidence. The following sections highlight key issues surrounding the identification and response to threats to IT and critical infrastructures and provide some balance to current threat discussions.

Current Threats

While each organisation is unique, any organisation, in its day-to-day operations, is likely to encounter a limited subset of threat agents responsible for nearly all successful and attempted intrusions against the organisation's infrastructures. These threat agents include insiders, industrial espionage and organised crime and structured and unstructured hackers.

Insiders

Recent survey results seem to indicate that insider threat is diminishing, though organisations should not rush to decrease spending on insider risk mitigation efforts just yet. The insider threat remains one of the most prescient in today's IT environment. While the survey indicates that insider incidents are decreasing, it is more likely that insider activity is being missed as organisations devote additional attention to monitoring their external environment and insiders become more adept at hiding their activities.

In addition to the disgruntled employee element of the insider threat, there is increasing concern regarding the use of insider placement as a penetration tactic. Organised threat agents, unable to penetrate external security mechanisms, will seek to place individuals within the organisation as temporary workers, employees or even as system administrators. It is important that a security programme implements safeguards to protect against insider threat. Such safeguards would include background checks for employees with access to critical systems, a recurring training and awareness programme to help employees identify and report potential insider incidents and implementation of internal security controls and network monitoring.

Placing insiders within an organisation is only one method of obtaining internal access to IT resources. In one example, an employee was found to have operated within several software development firms and was working for multiple companies and government agencies to develop custom software applications. In an era of distributed computing, additional vetting of subcontractors and support personnel and monitoring of internal network resources is required to counter this continuing threat.

Industrial Espionage and Organised Crime

Much has been written regarding the threat of industrial espionage conducted by both competitors and state-sponsored intelligence organisations. While industrial espionage is a continuing threat, it is one that many companies are familiar with and most attacks impact the confidentiality, not the availability, of the information. The sensitivity of business information will drive the safeguards required to protect its confidentiality and integrity.

Likewise, organised crime attacks are likely to exploit information for financial gain or to obtain access to sensitive information that is useful in the conduct of criminal enterprise. Critical infrastructure attacks do not fall within the operational purview of organised crime; however, we must remain open to the potential for organised crime entities to act as domestic proxies for terrorists or rogue nation states.

Structured and Unstructured Hackers

On a day-to-day basis, modern organisations are most likely to face threats from both structured and unstructured hackers. Scanning and probing of networks occurs on a daily basis against both specifically targeted and random systems. If an organisation is not encountering probing and attacks on a daily basis, its monitoring programme is not functioning correctly.

A recent study concluded that a vulnerable system connected to a public network would be compromised within 24 to 72 hours. The most common threat – the hacker threat – should be the easiest to counter and so, by ensuring that an organisation follows industry best practices for information security, it will be protecting itself from a majority of the attacks from this community.

It should be noted that a vital component of a best practice security programme will involve the monitoring of the 'white and black hat' hacker communities for information regarding new vulnerabilities that impact an environment. These communities, especially the white-hat community, serve as a vital and required red team for the software that runs critical infrastructures, and the vulnerabilities they discover could require immediate remediation and often involve issues of vendor accountability.

Countering Common Threats

The ability to counter these threats is a vital component to a diligent information security programme within an organisation. This demonstration of diligence also provides protection against the emerging threat of legal liability associated with IT security posture. Case studies are beginning to emerge where courts are taking actions to shut down IT infrastructures or hold organisations liable for their information security negligence.

Best practices for common threats are defined dynamically over time, and organisations must take the initiative to help ensure compliance. One of the best ways to validate efforts is through the use of indepen-dent threat and vulnerability assessments that document a security profile and establish recommendations for mitigating vulnerabilities or safeguarding from threats common to a particular industry.

Emerging Threats

In addition to handling the current threats adequately, risk management plans must also account for emerging threats such as terrorists and nation states. While most organisations are unlikely to face a threat from a nation state or terrorist organisation, those entities that qualify as critical infrastructures are attractive targets of attack. In fact, most private infrastructures are more attractive targets than government agencies or organisations.

Nation States

Conceptions of national security have adapted over recent years to include the attack and defence of the IT components of critical infrastructures. Numerous nations have developed programmes to facilitate this adaptation from both offensive and defensive perspectives. In congressional testimony, the director of the CIA acknowledged that over 100 nations are currently developing information warfare programmes in some capacity. The US is the most vulnerable to attack as it is the most reliant on IT. While this threat is real, the likelihood of a state-sponsored full-scale attack is low due to several factors.

First, most of the nations that are capable of launching an attack have highly interdependent relationships with the US economy. Any significant attack on the US will have economic consequences that are likely to impact the attacker substantially. In addition, a stated US policy allowing for conventional response to information warfare attacks serves as a deterrent for those nations looking to use information warfare attacks as an alternative to conventional warfare. However, it should be noted that these factors do little to deter a rogue state or nation using an information attack to gain strategic advantage within a conventional war theatre or to provoke a conventional response. Doctrine, coupled with the potential for anonymous attacks and a political environment where an anonymous attack is likely to be blamed on multinational terrorists, has caused slight modification of our evaluation of this threat. While it may be thought that this environment has made an anonymous, state-sponsored isolated infrastructure attack more likely, it is still felt that it would be with unsustainable or minimal consequences. In fact, the most likely consequences would be psychological and economic, two factors that can be controlled by adequately preparing response and recovery plans to accommodate the potential for these types of attacks.

Countering state-sponsored threats falls within the domain of the federal government. It is too costly for most private organisations to accommodate the potential for a nation state attack within their risk management structure without appropriate levels of intelligence being provided by the federal government.

In addition, it is within the realm of government responsibility to provide indicators to the private sector if they have evidence of an impending attack.

Terrorist Organisations

There are no strong indicators acknowledging that traditional terrorist groups will divert from conventional tactics to launch cyberterrorism attacks; however, the threat of cyberterrorism remains a high-profile concern. Despite the fact that there is a lack of solid open-source evidence supporting the notion of cyberterrorism attack, it should be viewed as a critical emerging threat for several reasons.

First, the ability to detect capability acquisition is severely limited due to the nature of the attack tools used. Given long-term planning cycles (three to five years for an attack in some cases), it is quite possible that a terrorist organisation is seeking to develop a capability for future attacks or that activity associated with existing capability acquisition has not been recognised. The proliferation of hacker tools that can be launched using a user-friendly graphical interface has also lowered the technical barrier required to obtain attack capabilities. In the past, these tools were not seen as having substantial impact against anything but Internet Protocol (IP) networks. However, in today's environment, some of the most critical infrastructures have been irresponsible when connected to public IP networks, making them susceptible to attack.

Second, it must be recognised that terrorist groups are being influenced by a younger, more technical membership and that they understand and use technology successfully in an operational capacity. There is evidence that terrorist organisations are seeking to gain education and training to use IT, but it is not clear if this is part of a programme to acquire a cyberterrorism capability or to support the infrastructure for logistics, planning and communication for future conventional attacks. However, given appropriate attention and resources, multinational terrorist organisations are capable of developing a critical infrastructure cyberterrorism attack capability.

Additionally, given constraints on physical travel, financial, logistical and support networks imposed on terrorist organisations through a co-operative war on terrorism, it becomes much more attractive to pursue cyber-attacks. The more successful we are at preventing physical terrorist attacks, the more attractive cyber-attacks become as they require no physical travel and can be launched simultaneously from distributed geographic locations. In fact, it is likely that attacks would be launched from geographic staging areas and compromised hosts to ensure that a conventional response to attack is not possible.

Finally, single-issue terrorist organisations have adopted cyberterrorism as a viable companion to continued physical attacks. Activists that specifically target IT infrastructures have also emerged and have launched isolated inconsequential 'hacktivist' attacks. As their level of sophistication and membership grows, they are likely to launch additional attacks. It is likely that any adoption of cyberterrorism by multinational terrorist organisations will be spearheaded by the successes of single-issue terrorists against isolated targets. Alternatively, a small cell of a multinational terrorist group may develop an attack concept that is pursued in parallel with planning for continued physical attacks or will conduct an attack to augment the impacts of a traditional attack.

Physical Threats to IT Systems

The reality of physical threats has been driven home by the events of 11 September 2001. When evaluating threats to an IT environment, it is important to recognise the viability of the physical threat and to evaluate the impact that a physical event would have on the continuity of business operations. Physical threats may manifest themselves in the wide range of attacks, from 'bomb' threats, causing the evacuation of a key facility, to large conventional truck bombs. The Terrorism Research Center's assessment methodology categorises over 100 types of physical attack, each with its own implications and impact. Physical attacks may be launched with the intention of impacting the infrastructure, not the general population, and contingencies for this type of attack must be developed.

Conclusion

In today's threat environment, a threat assessment methodology is a vital component of an organisation's security programme. This methodology should account for a wide variety of threats and should be based on realistic threat information projecting future threats while also accounting for previous experiences, incidents and documented attacks within an organisation's peer group. Threat assessments contain the following key components:

- description of the threat agent;
- likelihood of threat agent conducting an attack against the identified target;
- potential tools that the threat agent could use to attack the target;
- level of access the threat agent could obtain to use the tool against the target (should be based on actual results from vulnerability assessments); and
- potential impact an attack would have, including:
  - impact on operations,
  - cost of recovery and
  - intangible impacts such as loss of confidence.

To facilitate the use of the threat assessment within a risk management process, the methodology should also identify potential safeguards (with associated costs) and the reduction in exposure achieved through the implementation of the safeguard. Every attempt should be made to quantify the results of the threat assessment. Actionable items emerge from threat assessments that quantify exposure numerically, especially in terms of US dollars, as senior management can immediately relate to the potential exposure and the benefits of implementing a proposed safeguard. If a safeguard does not exist or is too costly to implement, contingency plans should be developed to facilitate response and recovery and minimise the potential impact from a successful attack.

In coming years, isolated attacks against critical infrastructures are likely to be experienced. However, the impact of these attacks can be minimised by planning appropriately for response and recovery. The Computer Security Institute (CSI) has noted that organisations will not be judged by how well they prevent an attack, but by how well prepared they are for it. Contingency planning for a full range of threats is a necessary component of those preparation activities

A threat assessment must be contained within a holistic security programme that includes appropriate policies and procedures, active assessment and recurring train-ing and awareness activities. It is also imperative that the level of information-sharing between the public and private sectors is increased. Unless private sector companies can utilise valid threat information in their risk management process, it is difficult to determine appropriate levels of spending to protect themselves. In addition, the fact that the most likely targets for a cyberterrorism attack are within the private sector means that, without information-sharing, the federal government has no insight to determine whether an event of national security consequence is occurring.

While this article identifies several current and emerging threats, additional analysis is required to validate the threat assumptions that are driving the risk management process. This article provides no discussion on the subject of attack tool/capability trends and this analysis is a required component of any organisation's threat assessment methodology. The threats to our infrastructures are real and very dynamic, and the ability to recognise and plan for them directly influences the impact of a potential attack. This must be done before those with the intent develop the capability or those with the capability develop the intent. ■

The full version of this article, including references, can be found in the Reference Section of the CD-ROM accompanying this business briefing.