2009

Ascent of Asymmetric Risk in Information Security: An InitialEvaluation.

Tobias Ruighaver
Deakin University

Matthew Warren
Deakin University

Atif Ahmad
University of Melbourne

Originally published in the Proceedings of the 10th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 1st-3rd December, 2009

The Ascent of Asymmetric Risk in Information Security: An Initial Evaluation.

Tobias Ruighaver[1], Matthew Warren[2] and Atif Ahmad[3]

[1,2]School of Information Systems,
Deakin University, Australia
[3]Department of Information Systems,
University of Melbourne, Australia

Abstract

Dramatic changes in the information security risk landscape over several decades have not yet been matched by similar changes in organizational information security, which is still mainly based on a mindset that security is achieved through extensive preventive controls. As a result, maintenance cost of information security is increasing rapidly, but this increased expenditure has not really made an attack more difficult. The opposite seems to be true, information security attacks have become easier to perpetrate and appear more like information warfare tactics. At the same time, the damage caused by a successful attack has increased significantly and may sometimes become critical to an organization. In this paper an extremely asymmetric risk is evaluated where a strongly motivated attacker unleashes a prolonged attack on an organization with the aim to do maximum damage. It is suggested that the probability of such an attack is increasing. The reason why preventive controls are unlikely to ever be effective against such an attack is discussed as well and proposals are made towards more advanced strategies that aim to limit the damage when such an attack occurs. One crucial lesson to be learned for those organizations that are dependent on their information security, such as critical infrastructure organizations, is the need to deny motivated attackers access to any information about the success of their attack. Successful deception in this area is likely to significantly reduce any potential escalation of the incident.

Keywords
Asymmetric risk, information security, information warfare.

INTRODUCTION

Over the past few decades organizations have become more and more dependent on advanced information systems to improve their business performance. As a result, these organizations' business continuity is increasingly relying on the security of their information technology and communication (ITC) infrastructure. Lately, organizations involved in critical infrastructure industries have also started to rely more on their ITC infrastructure to increase business performance. At the same time, the risk landscape for organizations that have to rely on more and more extensive and increasingly complex ITC infrastructures has changed dramatically as well. This paper suggests that organizational information security has been unable to keep up with these changes.

Our experience based on extensive case study based investigations into different aspects of security management in over 30 Australian organizations (Ruighaver 2007, Dojkovski 2007, Shedden 2006, Koh 2005) is that the current mindset in information security has stayed relatively unchanged since the 1980's. While recent security standards, such as ISO 27000 series (Humphreys 2005), have introduced a life cycle approach to information security, there is still mainly an emphasis on the management of individual risks through mainly preventive controls and there is a general lack of suggestions for a more strategic approach to information security.

The dramatic change in the risk landscape over the past few decades, as mentioned above, is not limited to a single aspect of information risk. A risk is generally identified as a threat impacting on a vulnerability resulting in an impact. Since the 1980's both the threat and vulnerability landscapes have evolved significantly, while the increased importance of information systems for organizations ensures that the potential impact of a security breach has become increasingly more damaging as well.

The next section discusses these changes and then focuses on the growing importance of certain asymmetric risks. While the use of asymmetric tactics in information security attacks is not new, there will be discussion on how changes in the motivation behind certain attacks, as well as the potential enormous impact of these attacks, makes it crucial that organizations identify these potential asymmetric risks and plan how they can reduce the impact of any security incidents resulting from such asymmetric risks.

The final section discusses why common incident response strategies may not be effective when these asymmetric risks eventuate and indicate potential research areas that need to be explored to generate new approaches to incident response.

THE CHANGING RISK LANDSCAPE.

The evolution of the risk landscape since the last century has not been limited to any single aspect of risk. This section discusses how there has been a significant increase in vulnerabilities as well as an increase in potential attack vectors - both crucial factors that increase the leverage of asymmetric tactics which will be discussed in the next section. Other changes in the risk landscape that have influenced the ascent of asymmetric risk, and will be discussed in this section, are a larger reliance on ITC infrastructure and the resulting increase in the potential impact of security attacks as well as a change in the fundamental motivation of some of the perpetrators.

The growing complexity of current ITC infrastructure, as well as the disappearing boundary between personal and business information technology, has lead to a dramatic increase in vulnerabilities that can be exploited by potential attackers. Many current security technologies, such as simple password based access control and some encryption based security solutions, have started to become obsolete as a result of the growing ease with which they become compromised (Ruighaver 2008). While companies are forced to invest in more complex security technologies, such as expensive virtual private networks and intrusion prevention systems, and are struggling to keep their systems up to date with the latest security patches, attackers can simply buy the latest attack tools from a growing number of providers in this new commercial industry.

At the same time, the potential impact of most security attacks is increasing as well. The larger reliance on ITC infrastructure means that a simple attack can force the shutdown of a crucial business system, or sometimes the whole company, even if that was not the main objective off the attack. Keeping copious amounts of sensitive data online or on a personal laptop often means that the impact of a confidentiality attack may result in the compromise of a whole database. Such attacks may have flow-on impacts such as a significant loss of reputation, as well.

While in the past hacking into a computer system was more or less a hobby, lately more professional groups of attackers have emerged. Organized crime has realized the potential financial gain that can be achieved by either blackmailing companies or by direct capitalization of a company's commercial data. Activist groups have realized the value of publicity that can be gained by crippling a company's web site. Organized groups of hackers in certain countries are actively engaged in information warfare.

> *…security professionals observing the state of the "hacker" underworld have long been very concerned about several significant factors likely to change the face of cybercrime within organizations. The first of these is the shift toward a "professionalization" of computer crime … Suffice it to say, though, that more of the perpetrators of current computer crime are motivated by money, not bragging rights.* (CSI Survey, 2007, p16)

Perhaps the most dangerous aspect of this change in the risk landscape is the change in motivation of potential attackers. While the primary objective of an attack may not be to inflict maximum damage, a potential attacker is now rarely satisfied by compromising security alone. As a result some attacks have been prolonged creating progressive amounts of damage in subsequent phases of the attack.

ASYMMETRIC TACTICS

An important, but not the only aspect of asymmetry in risk is the asymmetry of the threat. An asymmetric threat is any threat that is disproportionate in its impact. In physical security the asymmetry is often in the size of the attackers and defenders, for instance when a small group attacks a large target. An example of such an asymmetric threat is that of terrorist attacks. An example of a small group attacking a large entity, in this case a country, were the attacks carried out on the World Trade Center on September 11th, 2001. The perpetrators of this asymmetric

attack were a group of individuals with different nationalities and a common cause. About 20 of them ended up killing over 5,300 - the ratio being 1:250. While the asymmetric attack using a small attack force is not new, and has been used for many years with varying success, the problem in information security is not necessarily related to the size of the attacker or defender.

In information security there are two dimensions that differentiate modern asymmetric threats from traditional threats. Firstly, the amount of effort and resources that has been expended by the attacking entity is small, whereas the corresponding impact of the attack on the defending party can be described as 'overwhelming'. This dimension can be called 'leverage' as it signifies the ratio of the input by the attacking party compared to the output gained by perpetrating the particular type of threat. The second dimension is the motivation of the attacking party. Previous motivations of attackers on the Internet have been described as 'bragging rights'. A recent shift has seen more profound reasons emerge that fall in categories such as adherence to an ideology or pursuit of financial benefit.

This change in motivation has necessitated a consequential change in operational tactics. In this paper, the resulting tactics are called 'asymmetric tactics'. Rather than using the past 'shotgun style' attacks where large numbers of Internet Protocol addresses are probed and then investigated for vulnerabilities, individual targets are pursued with a range of attack vectors in the hope that the objective (which is frequently to incapacitate the target organization) is achieved. In this way, modern asymmetric threats appear to be conducting 'information warfare'. Also, since attackers are more focused on the objective of the attack, they are more willing to engage the defending party for a prolonged period of time, until the objective has been achieved.

Unfortunately, from the defender's point of view, the number of potential attackers using asymmetric tactics will increase dramatically because the level of competence required to carry out these attacks (which was previously enough of an impediment to limit the number of potential attackers and attacks) has decreased with the large-scale availability of sophisticated tools. While this is not a new trend at all the commercial marketing of these tools over the past few years has lead to their wide spread distribution. And, each time a new advancement in security is publicized the people that are selling these attack tools spend their time working out how to overcome these obstacles. Often they succeed updating their tools before many of the organizations that need to protect themselves have had a chance to implement these new security measures and patches.

The long-standing mindset of many organizations, which relies on largely preventive measures to keep out potential attackers, is no longer cost-effective with the rise of asymmetric tactics. A number of recent cases have demonstrated how asymmetric tactics can be used to simply overwhelm the defenses of organizations. In such scenarios, incident response teams are helpless as there are too many attack vectors and vulnerabilities to address in a very short time-frame.

In this case, organizations may be better off going underground and protecting their core business function with the aim of surviving the storm until it is safe to re-emerge.

All the power of a nation state cannot deal with the speed and stealth of a sophisticated and motivated team mounting an asymmetric attack. Hence, in the war against terrorism the emphasis has mostly been on forensic investigations following each terrorism attack and on the surveillance of potential attackers and early detection of potential new attacks. Incident response to an asymmetric attack itself only plays a minor role, but planning the hardening of potential targets has often lead to a significant reduction of damage of terrorism attacks.

The use of asymmetric tactics on critical infrastructure targets creates potentially even more problems given much of it is controlled either by computers themselves or by human input into computers. And in particular over the past few decades a nexus has developed between infrastructures that have changed the security landscape within which modern society operates. For example, interdependence between telecommunications and electricity networks has created a security environment where events originating in one infrastructure can have direct impact on another and vice versa. (Dunlevy 2004). Hence, asymmetric information warfare tactics can, and sometimes already have been, successfully used against:

- Telecommunications Networks
- Electrical Power Systems
- Banking and Finance
- Water Supply Systems
- Transportation Networks

- Emergency Services

All these services use Information Systems to some extent for control purposes. If control was diverted or subverted for any of these services it could be catastrophic for an organization or potentially even for a country. At present the telecommunications and electricity supplies are the most important infrastructures that keep our information systems working. If either of these were to be interrupted for a lengthy period it would have catastrophic repercussions.

While the disruption of our power supply potentially cripples our information systems, many organizations are currently already trying to remedy this through the use of portable workstations and the use of alternate power sources for their servers. This will allow their employees to continue to work as long as telecommunications are not interrupted. What is more difficult to protect against is the potential panic and general disruption that a successful attack on our power supplies might generate. This will potentially lead to an overload of communication and helpdesk services.

With the disruption of our telecommunication networks again our information systems will be crippled. And although the process has already begun to avoid this from happening by the use of wireless communication infrastructures, this solution is by no means full proof. Furthermore, the use of wireless communications will enable other asymmetric attacks. At each turn and with every new innovation there are new risks associated.

ASYMMETRIC RISK.

The growing use of asymmetric tactics is only one aspect of the ascent of asymmetric risk. The real problem is the increased impact that such an asymmetric attack can now have on an organization or on a country. Hence the use of asymmetric tactics is only one aspect of asymmetry. With so many essential functions of modern life revolving around the information systems in this post-industrial age, society is subject to a whole new meaning of the term asymmetric risk. And the probability that such an asymmetric risk will occur is still growing.

Therefore a critical asymmetric risk in the information systems area is defined as any risk that has a potential critical impact on an organizations business processes and can be caused by low capability attackers with minimal effort even though the organization has put a reasonable effort into avoiding or mitigating that risk. As discussed before, this paper is concerned with critical asymmetric risks caused by motivated attackers who are willing to sustain prolonged attacks. A few examples of where these asymmetric risks could come from may help here.

- Disgruntled employee's, especially Information Technology personnel,
- Terrorists,
- Religious Groups,
- Political Groups.

To illustrate the importance of asymmetric risk for current information security, a recent incident will be now discussed more extensively: In 2009 the Melbourne International Film Festival (MIFF) showed a documentary about Rebiya Kadeer called "The 10 Conditions of Love". The Chinese government asked the film festival organisers to withdraw the film, since they accused the exiled Uighur leader Rebiya Kadeer of plotting Uighur riots in China (News.Com.Au, 2009). The festival organizers ignored this request and what followed was a sustained attack on the organization. It is unclear how much the Chinese government supported or encouraged this attack.

The stages of the resulting security incident are:

Phase 1 – Email Phase

The first phase of the incident related to sending emails to film festival staff, to make them change their mind regarding the showing of the film. The festival director reported that "the language has been vile, it is obviously a concerted campaign to get us because we've refused to comply with the Chinese Government's demands" (News.com.au, 2009).

Phase 2 – Hacking Attack

Hackers broke into the festival's website early yesterday (30th July), just hours after Victorian Premier John Brumby officially opened the 2009 festival at the Arts Centre. The hackers replaced festival information with the Chinese flag and anti-Kadeer slogans (The Age, 2009a) as shown in Figure 1.

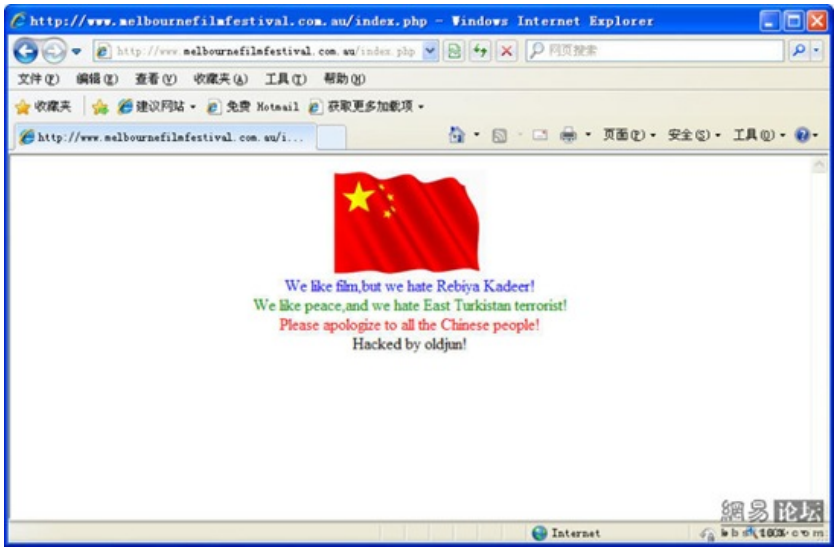

Figure 1: Hacked Screen Shot of Festival (Chinahush, 2009)

The Melbourne International Arts Festival web site was also hacked and a similar message as described in Figure 1 was left on their, web-site. The Melbourne International Arts Festival had no connection with Rebiya Kadeer and was perceived as being hacked by mistake (The Age, 2009b).

Phase 3 – Denial of Service Attack

The MIFF online ticketing experienced Denial of Service attacks from unauthorised sources. Some of these attacks came from offshore and some came from within Australia (Melbourne International Film Festival, 2009a). According to MIFF, their web site had 80,000 hits per day compared to the usual number of 10,000 hits per day (Techworld, 2009). The impact of the attacks was that users of the MIFF website may experience slower than normal response times (MIFF, 2009b).

Phase 4 – Disruption Attack

Organisers of the Melbourne International Film Festival were forced to shut down its online ticket sales system after 'Chinese hackers' booked out all film sessions on its website When the bookings were traced to Chinese websites and they were identified as being fake (News.com.au, 2009). The outcome of the attack was that MIFF online ticketing website was fully functional, but only existing customers could use the systems, customers had to log in using their existing email address and password (MIFF, 2009c).

Instruction of how to manipulate the Melbourne International Film Festival were emailed via the Internet, the email provides instructions for loading tickets into 'shopping carts' from the festival's website, and Chinese were being urged to teach others how to "purchase" MIFF tickets online (Sydney Morning Herald, 2009).

The overall attacks went from stages 1 to stage 4 occurred over a ten day period (BBC, 2009).

DEFENSIVE STRATEGIES TO MITIGATE ASYMMETRIC RISK.

The traditional approach to information security as supported by the current security standards is heavily dominated by the use of preventive controls and relies on the implementation of an expensive security management system to maintain its effectiveness. As discussed earlier, the increased complexity of both the ITC infrastructure and its technical security controls means that this traditional approach is not likely to be effective against an attacker using

asymmetric tactics. Furthermore, this extensive use of preventive controls makes it easy for an attacker to evaluate the success of his attack and choose an alternative attack scenario if the attack is not completely successful.

Traditional incident response philosophy has been developed towards response to a single attack and is likely to be overwhelmed when a motivated attacker unleashes prolonged and multi-pronged attacks. This situation is further complicated when the incident response team is faced by a continuing attack and cannot easily decide when the attack will finally end. The role of incident response in such an attack is discussed later in this section.

Organizations that are part of a country's critical infrastructure are expected to spend at least some resources on the direct defense against asymmetric attacks. Other organizations may not be able to afford extensive investments in direct defense, but will need to plan their response to limit the damage and ensure business continuity (Hiles 2001) if a prolonged asymmetric attack occurs. Business continuity will be discussed at the end of this section.

The standard approach to limiting the damage from an attack is based on compartmentalization. This approach may potentially also be successful in limiting the damage from an asymmetric attack if a traditional Defense-in-Depth (DiD) strategy is applied. The initial aim of Defense-in-Depth is to delay an attacker while he is concentrating on your first defensive line, so you can deploy defensive countermeasures to protect your next line of defense. Such defensive countermeasures can consist of a complete isolation of the compartment that is under attack (as in a perimeter network firewall) or they can be more subtle and advanced.

It is important to realize that a response to an asymmetric attack needs to be within the timeframe of the attacker. If an attacker has breached one compartment, then there must be a response before resources in the compromised compartment can be used to attack another compartment. That means that in most cases some automated form of response is needed. As such an automated response will in general cause some damage (e.g. isolation is a form of Denial of Service) it is important that these responses are well planned and approved at the highest level.

To enable an effective response, it is important that surveillance is increased in other compartments when the initial attack is detected. While an attacker is able to focus his attack on a few assets, the defender will need to protect all assets. The earlier the defender recognizes whether asymmetric tactics are being used, and which compartments are in danger of being compromised, the more effective the response will be.

A very advanced and potentially extremely effective strategy to augment Defense-in-Depth is the use of deception. If it is detected that an attacker is using asymmetric tactics, it becomes crucial to deny the attacker access to any feedback on the success of the attack. Deception, such as redirection of the attack to a honeypot, can be used to mislead and confuse the attacker. Deception is still an underused strategy, it is important that new research in deception as a countermeasure is encouraged to combat the ascent of asymmetric risk.

Incident response and business continuity are traditionally not closely coupled. The increased probability of extreme asymmetric risks that can have a dramatic impact on critical business processes will mean that more emphasis is needed on business continuity during incident response (because of the potential of extreme impact). At the same time, standard business continuity plans such as moving from a primary site to a secondary site, are not necessarily effective in this situation especially if the attack is aimed at an Internet Protocol address rather than a physical location. So new business continuity plans will need to be developed to ensure core critical business processes can still continue. Planning the diversification of critical business processes before such an attack takes place can greatly assist an effective response to a prolonged asymmetric attack, allowing some business processes to go "underground".

CONCLUSION

The continued deterioration of the risk landscape for Information Technology and Communication infrastructures, and the increased reliance of organizations on their ITC infrastructure, has lead to an increased likelihood of extreme asymmetric risks impacting on an organization's critical business processes. Organizations can no longer safely ignore or accept these risks and will need to start planning strategies to reduce the impact when these asymmetric risks eventuate. While the strategies proposed in this paper are particularly relevant for any organization involved in a country's critical infrastructure, other organizations will need to be aware that they can no longer ignore these risks either.

The particular asymmetric risks discussed in this paper are difficult to defend against using current security approaches, even when an organization is willing to seriously invest in preventive security controls and traditional incident response capabilities. For organizations facing information warfare tactics used by a motivated attacker several new strategies are proposed to limit damage. The need to integrate new business continuity responses in an organization's incident response planning is also discussed. This paper has not been limited to particular (detailed) asymmetric attack scenarios, it is believed that the proposed approach to mitigate these extreme asymmetric risks will lead to a flexible and adaptive security posture that will increase the organization's overall information security for a range of other attacks as well.

Future research by the authors in this area is an extension of their current research in how organizations develop new strategies, a concept called security strategic context, to cope with their deteriorating information security. The authors are currently planning a focus group based research study to investigate the relationship between the development of new information security approaches and an organization's culture of change. In particular, the authors are interested in what factors might influence the introduction of the strategies proposed in this paper.

REFERENCES

BBC. (2009) Chinese hack film festival site. Retrieved October 11, 2009, from http://news.bbc.co.uk/2/hi/8169123.stm

ChinaHush. (2009) Chinese Hackers Hacked Melbourne Film Festival Website, Again. Retrieved October 11, 2009, from http://www.chinahush.com/2009/08/02/chinese-hackers-hacked-melbourne-film-festival-website-again/

Dojkovski, S., Lichtenstein, S. & Warren, M. (2007) Developing Information Security Culture in Small and Medium Size Enterprises: Australian Case Studies, *Proceedings of the 6th European Conference on Information Warfare and Security*, CD-ROM, Academic Conferences Limited, United Kingdom

Hiles, A., Barnes, P. (2001) *The Definitive Handbook of Business Continuity Management*, John Wiley & Sons, Chichester.

Humphreys, T. (2005) State-of-the-art information security management system with ISO/IEC 27001:2005. ISO Management Systems.

Koh, K., Ruighaver, A.B., Maynard, S.B., Ahmad, A., Security Governance: Its Impact on Security Culture, *Proceedings of the 3rd Australian Information Security Management Conference*, Perth, Sep 30, 2005.

Melbourne International Film Festival (2009a) Press release: MIFF Ticketing Statement. Retrieved October 10, 2009, from, http://www.melbournefilmfestival.com.au/content/57/newsitem/161.html.

Melbourne International Film Festival (2009b) Press release: MIFF Website Issues, Retrieved October 10, 2009 http://www.melbournefilmfestival.com.au/content/57/news.html

Melbourne International Film Festival (2009c) Press release: WEBSITE DISRUPTION. Retrieved October 10, 2009, from, http://www.melbournefilmfestival.com.au/content/57/news.html

Ruighaver, A.B., Maynard, S. & Chang, S. (2007) Organizational Security Culture: Extending the End-User Perspective, *Computers & Security*, *26*(1), 56-62.

Ruighaver A.B. (2008) Organisational security requirements: An agile approach to Ubiquitous Information Security, *Proceedings of the 6th Australian Information Security Management Conference*, Perth, Dec 2008.

Shedden, P., Ruighaver, A.B. & Ahmad, A., (2006) Risk Management Standards - The Perception of Ease of Use. *5th Security Conference*, April 19-20 2006 Las Vegas, USA.

COPYRIGHT