Free InfoSec Training, Compliments of History

Chris Bachmann
September 21, 2001
GSEC – V1.2f

On May 24, 1941, the German battleship Bismarck, one of the largest and most sophisticated battleships created to date, was attacked by Swordfish biplane torpedo bombers from the aircraft carrier Victorious. Since these planes were outdated relics of WW I, none of the pilots expected to come back alive from what was an apparent suicide mission. However, every single one returned safely. Post analysis showed that the sophisticated deck guns of the Bismarck, with their advanced tracking mechanisms, were never designed to target something moving that slow.

Between 1929 and 1940, the French created the Maginot Line, a heavily fortified border between themselves and Germany. However, when the German forces invaded Belgium to the North and carried south into France through the "impenetrable" Ardennes Forrest, the defense mechanism failed. The larger failure was the "Maginot Mentality" in France at the time, a sense of false security behind a single defensive mechanism.

If the topic is Information Security, then why are we citing and detailing historical incidents? Simple. We are all soldiers in a war to guard assets against attack and as any good military leader knows, those that are unaware of history are doomed to repeat it. How many of us fortify ourselves with technology like the Bismarck, only to get defeated by a low technology attacker, perhaps utilizing social engineering or a simple SYN flood? Are we ever victims of the Maginot Mentality, forgetting that Napster, Gnutella and modems left on auto-answer allow a simple way to circumvent firewall security? Are we at least using egress filtering of FTP to add an additional layer of security toward an enemy that may already be behind our lines, or are all of our defenses aimed outward? Even if we fully understand these issues, how do we express the need for budget to a manager that feels perfectly safe utilizing the corporate firewall as a single line of defense?

In this paper, I will attempt to accomplish the following:

1) Demonstrate how historical lessons can improve our skills as InfoSec professionals

2) Demonstrate how historical lessons can be used as a platform for management to understand the technology solutions we are proposing

In our profession, we are all guilty at times of developing tunnel vision, getting caught up in budgets or examining the latest technology. Beyond our planning and analysis, we have the added requirement of expressing to management, in terms they can understand, why our security recommendations should be heeded. History allows us to step back and stay focused on the core essence of our jobs, guarding assets. It can also allow us to establish precedent with management as to why our recommendations should be heeded. Technology will change with time but the principles and lessons remain the same. It is upon these principles we will fight and win our battles.

For those of you examining history for the first time, you will notice that there is an awful lot of it. For this reason, we will narrow our focus to a single series of events. We are going to examine the September 11, 2001 terrorist attacks on the United States, the events leading up to them and the resulting actions taken. This will be done through the eyes of an Information Security Professional looking to gain insight into performing his job better.

Before the Attacks

In 1995, Philippine police investigating an apartment fire discovered it to be the hideout of Ramzi Yousef and Abdul Hakim Murad, international terrorists. The Philippine authorities captured Murad but Ramzi escaped, only to be later captured and convicted for his involvement in the 1993 World Trade Center bombing. During questioning, Murad related plans to hijack commercial airlines in the continental United States and crash them into CIA HQ in Langley, VA and the Pentagon. Later investigations also showed plans to target commercial towers in New York, San Francisco and Chicago. This information was turned over to the FBI.

> Lesson: Credible threats don't always mean imminent danger. Often, we have time to create an infrastructure to eliminate the threat by the time it manifests, if we don't ignore the warnings. For example, at the current pace of technology, how secure are DES, 3DES and AES? Continuing development of better encryption standards will always be necessary to stay a step ahead of even simple brute force attacks with faster processor speeds.

We are all aware of airport security issues. 60 Minutes has done undercover work several times to show how easy it is to get into secure areas such as the tarmac with false or even worse, no IDs at all. Stories have spread through the media for years and the United States continued to maintain what was best described as lax security.

> Lesson: Often, vulnerabilities are common knowledge to the "good guys" as well as the "bad guys". Companies are often guilty of ignoring the obvious and seem surprised when an attack occurs. Most attacks occur by utilizing vulnerabilities that are common knowledge. Prevention can be as simple as applying a readily available patch.

The FAA claims a 95% effective security level. This is a result of FAA inspections featuring such benefits as pre-announced audits and the use of obvious materials in otherwise empty gym bags. For years however, the Red Team, a specialized unit belonging to the FAA's office of Civil Aviation Security, has conducted covert airport security checks with a success rate in excess of 90% in bringing simulated weapons and bombs onto planes, the exact inverse of the FAA's announced security level. In 1998, to get objective results, Cathal Flynn, the FAA's deputy administrator for security, contracted an external firm to conduct covert vulnerability assessments of major US airports. Of 450 tests, the team was only caught 4 times.

> Lesson: Tests can always show a desired result when staged properly. However, true vulnerability tests are conducted in a live environment. More importantly, if those in a position of authority are not prepared to act on the findings, the results are useless. A large part of our job focuses on properly conveying to those in authority the threat and the cost analysis of addressing the threat. This example should offer our management a clearer understanding of the value of conducting and more importantly, acting upon vulnerability studies. If those in authority had seen the financial and social repercussions of the September 11th attack 5 years ago, would airport security have been increased by now?

Security officers were on duty as usual at the front desk of the World Trade Center buildings the morning of September 11th. No one questions their security skills, policies or training. However, at airports miles away, far outside their span of control, lax security allowed a dangerous and lethal situation to develop. As a result, the only security measures that were of use were evacuation protocols. None of their security measures could compensate for the lack of security elsewhere.

> Lesson: Like it or not, we are all in this together. Threats to us may result from lax security on someone else's part, as in the case of a DDoS. We can have the best security policies, training and personnel and still be vulnerable as a result of someone else's negligence. Or, from the airline perspective, we may be the weakest link and the cause of loss to others if we are not diligent. It is only through increased security and the sharing of best practices on all fronts do we raise the cumulative security of the whole. The concept of "not my company, not my problem" is incorrect, ignorant and irresponsible.

During the Attacks

On the morning of September 11, 2001, highjackers took over 4 separate flights wielding only box cutter knives.

> Lesson: Many times, incidents are a result of low-tech methods such as social engineering or plain deception. We solidify our perimeter with technology such as badge access control but the attacker walks in by tailgating behind a real employee.

The blades on the knives used by the highjackers were well within regulation for carry on items, yet they were more than effective in allowing them to achieve their objectives.

> Lesson: Clear and thought-out policies are essential to effective security. Even the strictest enforcement of policy will be useless if we fail to periodically review and reconsider exactly what we are enforcing. However, just as the United States must balance additional security with civil liberties, so too we must balance security with employee privileges. A citizen may not leave the country if no longer allowed to carry a shaving razor onto a flight for an overnight trip, but an employee may certainly consider leaving the company if they consider security policy to be prohibitive or intrusive.

At ground zero, New York Fire Fighters and Policemen raced to contain the incident by cordoning off increasingly large areas as buildings began to fall. They followed their training and attempted to minimize losses by assisting in the evacuation of the buildings. The Federal Emergency Management Agency, Army Corp of Engineers, National Guard and the Center for Disease Control have all mobilized to do their part in the massive effort to contain the damage and recover from this situation. Despite the overwhelming nature of the task and the hundreds of people operating in parallel, efforts continue to be described as well coordinated and effective.

> Lesson: During an incident, especially a critical one, is not the time to decide who should be involved and what role they should play. Responsibilities need to be clearly defined, written and rehearsed. Only then can you hope for an efficient and effective handling of an incident. This is not news to a security professional, but it may serve as an excellent example to management as to why drills should be run that include Human Resources, Information Technology, Legal, Management and Security Team personnel?

In a timely fashion, the Federal Aviation Administration alerted NORAD's Northeast Air Defense Sector in Rome, N.Y. as they became aware of each of the 4 separate flights that had been hijacked. In each case, F-15 and F-16 fighter jets were dispatched to intercept. The president was in contact with his staff and specifically Vice President Cheney. After the attack on the Pentagon, President Bush authorized fighters to shoot down planes that threatened targets in Washington in an attempt to minimize additional loss. Though the orders never needed to be carried out, the communication channel worked and the proper authority was in touch with the correct resources to make a timely decision.

> Lesson: Admittedly, the fighters arrived too late. However, this still stands as a great example of something that went right. In an emergency, it must be immediately clear whom to contact. Policy on how to respond to a given threat must be understood by the incident response team so the reaction is swift and professional, not flustered and hurried. More importantly, it must be clearly identified who has the authority to enact certain measures and the responsibility of living with those decisions. Do you want an F-16 pilot to make the call on shooting down a passenger jet with civilians aboard? Do you want a web

administrator to make the call on taking down an e-commerce web site as a result of an incident if she feels that additional data is at risk? These might be viewed as career-limiting events without proper authority. Clearly identify in written policy what authority is carried by whom.

Results of the Attacks

In the United States, airports are now increasing security measures. Entire airports were closed pending FAA security review, baggage is being checked by hand and only ticketed passengers are allowed to the gate areas. Security in airports around the world are also being increased or at least further scrutinized.

> Lesson: It is amazing how measures declined before an incident will often become more acceptable post-incident, even if additional budget is required. Some executives are not aware of how credible certain threats are and how much damage they may inflict, despite our best efforts to help them understand. As professionals, we should calmly utilize a post-incident period to examine and enact additional security measures that may have been declined before. Documentation will also be key. Do you think the head of the FAA had written documentation to Washington on the dangers that may result from lax security prior to this incident? While management may not put budget toward items we consider necessary from a security standpoint, it is still their decision to make. However, this does not mean that the security professional should be held responsible for the results of that decision.

Companies in the World Trade Center buildings lost employees, data, systems, and for some, the physical ability to continue. For example, Cantor Fitzgerald, which occupied floors 101-105 of One World Trade Center, has over 700 employees dead or missing. The CEO has pledged 25% of their bond trading profits to help the families of those lost but the company may fail as a result of the incident.

> Lesson: Though unlikely, the unthinkable can happen. Complete loss may come in a form as unlikely as a terrorist attack or in the more likely form of a disaster such as a fire, flood or hurricane. A comprehensive disaster recovery plan must include elements for data, systems, facilities and skills. We need to keep in mind that our planning ensures not only the continuity of the business but also the continuity of livelihood for our employees and their families as well.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles." This is a famous quote from the military strategist Sun Tzu in his treatise, The Art of War. Though written over 2500 years ago, it still holds true today. At this time, the United States faces a potential enemy being harbored in Afghanistan. According to authoritative reports, the CIA has no agents in the field in this country and the view from a satellite offers little useful information. Diplomatic and military efforts are underway to gather the necessary information to be successful in this campaign. This information includes religious, political, ethnic, regional, social and financial information on the enemy we face. We need to understand how they think, act, plan and move to be successful.

> Lesson: Such is true in information security. The only way to successfully guard something is to truly understand those that would take it away from you. By understanding how hackers and data thieves think, act and move, you will be much more successful in guarding against these attacks. Books such as Steal This Computer Book by Wallace Wang show things from a hacker's perspective. It is also a great source of information on hacker websites, magazines, newsgroups and even conventions. Hackers regularly scan your systems for information to be successful. You should return the favor. If someone in your organization is not periodically collecting reconnaissance data from these sources, you will lose.

There will be those who claim that things are different today and that technology has changed everything. Julius Caesar utilized encryption and computers hadn't been invented. In the words of Sun Tzu, "What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge." This demonstrates a clear understanding of the value and necessity of intelligence gathering, even though satellites weren't orbiting the earth yet. Tools may change but the concepts remain the same.

This article was written and submitted on September 25, 2001. As such, many people will say that it was timely. If you are one of these people, you have entirely missed the point and I urge you to read it once again. This article and the lessons contained are not timely; rather they are timeless. They are free InfoSec lessons, compliments of history.

References

1. CBS News, "How secure are our airports?", September 17, 2001.
URL: http://www.cbsnews.com/now/story/0,1597,311591-412,00.shtml

2. Rashid, Ahmed, "US Lacks knowledge to start land war", September 19, 2001.
URL:
http://www.portal.telegraph.co.uk/news/main.jhtml?xml=/news/2001/09/19/wwar19.xml

3. Ressa, Maria, "US Warned in 1995 of plot to hijack planes, attack buildings", September 18, 2001.
URL: http://www.cnn.com/2001/US/09/18/inv.hijacking.philippines/index.html

4. DiGiulian, Tony, "What destroyed the Hood?", updated February 1, 2000.

URL: http://www.warships1.com/BRbc15_Hood_loss.htm

5. Associated Press, “Fighters were 8 minutes away from WTC”, September 19, 2001.
URL: http://www.washingtonpost.com/wp-srv/aponline/20010919/aponline091804_000.htm

6. Donnell, C&D, “Brief history of the Maginot Line”, copyright 1997 to 2001.
URL: http://www.geocities.com/Athens/Forum/1491/pagetwo.html

7. Garzke Jr., William H., “Bismarck’s Final Battle”, 1994.
URL: http://www.warships1.com/W-INRO/INRO_Bismarck_p1.htm

8. Sun Tzu, “The Art of War” (Originally written about 500 B.C.), Translated from Chinese by Lionel Giles, M.A. (1910), Edited by James Clavell (1983).

9. Wang, Wallace, “Steal This Computer Book 2”, No Starch Press, Copyright 2001.