



Protecting Your Information Assets - What Hackers Know That You Don't

Abstract

Security is a never ending game. The playing field is your information system. Your goal is balancing two separate balls. One is your ease of access, storing, and transmitting data. The other is ensuring information confidentiality, availability, and integrity. Some of your adversaries have actually been on your own team, such as current and past employees. Other adversaries have been on the opposing team, such as your competitors. Hidden adversaries, such as hackers, lie in wait on your playing field. All of your adversaries want your valuable data and are willing to play the game to get it. What you don't know is that your adversaries don't play by the rules.

Why do intruders hack into systems? Think of your information system as an electronic maze or crossword puzzle. It is a challenge to a young mind to break in and win the game. In today's world, information systems are the game and your data is the prize. You win the game by keeping intruders out of your system. Intruders win the game by breaking into your system.

This paper addresses what hackers know that you don't and what you need to do to win the game by protecting your information assets.

The Players

For the purposes of the game, we introduce the players:

- Information – your team's data that is electronically stored and communicated.
- Information assets – information that has value to your team.
- Information security – ensures the confidentiality, availability, and/or integrity of your team's information assets.
- Intruder (hacker) – an adversary who affects the confidentiality, availability, and/or integrity of your team's information assets.

Your Team

In playing the game, your team knows the value of information and the importance of identifying and protecting your assets. Information assets, whether tangible or intangible, are essential to your team's well being. These assets are necessary for day-to-day operations and must be protected to ensure the survival of your team and its ability to provide products and services.

Your team's information may exist in many forms. What may be sensitive or important to one team may not have the same relative value or importance to



another. Threats to information assets depend on varying circumstances including:

- Confidentiality – ensuring the proprietary nature of information is protected and can only be read by authorized users or programs.
- Availability – ensuring information is available in the required time frame.
- Integrity – ensuring data is only altered or destroyed in an authorized manner.

Opportunities to compromise information assets amplify as your team uses:

- Remote connectivity – remote locations frequently do not have the same types of security systems in place as found at corporate offices and on the main playing field.
- Mobility – as electronic organizers and personal digital assistants (PDA) replace traditional Day Timers, mobile information devices put data on the move. Data is harder to secure as your team transitions from a stationary space to a mobile platform.

By providing remote access to data, your team presents additional opportunities for intruders to gain access to your team's information systems.

Your Win Loss Record

On the playing field of your information system, your goal is to balance access to information versus the risks associated with providing that information. Employee remote access, mobile information devices, hard drives in office copiers, and new technology developments are all risks your team faces.

Risk is related to the probability of the compromising event and the impact of the compromise to your team. If either the probability is high or the impact is high, then your risk is high.

Security protection costs should be directly related to the impact on your team if your data is compromised. Not all data is valued the same and some data is more valuable than others. If you want to win the game, you need security controls and procedures to protect against intruders.

Preparing a Strong Defense

Your strongest defense is effective risk management. Effective risk management is a significant undertaking and security systems can only be as strong as the weakest team member. One way to reduce risks is by securing information assets. Risk analysis and planning protects information assets from compromises in the areas of confidentiality, integrity, and availability. The importance of confidentiality and availability may vary from one team to another. Most teams, however, find data integrity an essential element of information security. Without data integrity, information is of little value to the team.



Information systems are like a strong defense. They need sufficient security procedures and controls to protect the team's information assets from intruders.

Your Team Leader

The first step to securing information is to identify and prioritize the assets that are important to the team. The team should identify how the data might be compromised and the resulting impact to the team if the data is compromised. Once your team has identified its information assets, relative importance, threats, and impact, you team can determine risk tolerance and implement the appropriate security controls.

A Single Point Of Failure (SPOF) or business impact analysis helps determine the impact to a team should the confidentiality, availability, or integrity of data be compromised. A SPOF analysis examines the impact of the failure of a system to perform its function. Security systems, for example, may fail and allow an intruder access to financial data. What is the impact to the team over time? What departments are impacted? How does the failure of a security system affect the team's image and reputation?

A SPOF analysis helps allocate security resources so information assets and equipment are protected from intruders according to the importance of the information to your team.

Your Hidden Adversary

The more information your team has about intruders and their types of attacks, the more successful your team can be at guarding against loss of data. High school and college students, Generation Y born 1978 through 1995, have access to the knowledge and time needed to be a threat.

What we know about Generation Y ^{1, 2}:

- Generation Y composes 21% of the population of the United States and, at their peak, will exceed the number of baby boomers by at least 5% ³.
- Generation Y is often called "Digital in Diapers", they have always had digital equipment including cell phones, e-mail, and PCs ⁴.
- 81% of ages 12-17 use email, 70% use instant message to keep in touch with friends and relatives, and 56% of ages 18-19 prefer internet to telephone⁵.
- 96% of the Generation Y population estimates they will be between 30 and 40 years old when they make their first million dollars.
- 73% of Generation Y want a job where they can set their own work hours.
- For their first job, Generation Y workers want a fun atmosphere.
- Generation Y workers will typically have seven jobs in their career.
- Generation Y workers are not concerned about the corporate ladder.
- Generation Y requires constant stimulation.



- Baby Boomers will spend approximately 5 ½ years on-line over their lifetime. Generation Y workers will spend more than 23 years of their lives on-line⁶.

Generation Y is willing to take more risks and be more aggressive online than they ever would in person⁷. Successful intruders do not require substantial sums of money. Knowledge, time, and a constant desire for stimulation are the trademarks of a Generation Y intruder. Not all intruders are equal. Experts believe that for every 100,000 novice intruders there are:

- 5,000 intermediate level intruders with some form of computing experience, and
- 1,000 elite intruders capable of penetrating most systems

Intruders Seek Opportunities

Intruders know to look for opportunities. The facts are simple, the greater the number of workstations and equipment, the greater the likelihood a vulnerability exists. Workstation estimates ⁸:

- 39% of teams have less than 499 workstations
- 20% of teams have 500 to 1,999 workstations
- 22% of teams have 2,000 to 10,000 workstations
- 19% of teams have more than 10,000 workstations

Time is on the side of the intruder. It is only a matter of time before an intruder can identify an opportunity. Intruders know that opportunities exist:

- Intruders use people, scripts, and viruses to probe for security vulnerabilities.
- Intruders identify weaknesses in operating systems, application software, and configuration errors.
- Teams create opportunities for intruders by leaving systems un-patched when fixes are available.
- Intruders know teams have time constraints and can not secure everything.

Access to Your Playing Field

Intruders know that many systems are only secured by a password. With a simple and easy to guess user id, all an intruder needs is a password. Intruders know:

- Users like easy to remember passwords that provide access to all of their data. Once one password is compromised, an intruder gains access to multiple systems.
- Users write down hard to remember passwords. These passwords are frequently stored near their computer system. Intruders know that by gaining physical access to the workstation, they may find passwords on Post-it notes, under the keyboard, etc.
- Users do not like to change passwords. Once a password is obtained, the intruder has weeks or months before it expires.



- Most passwords are simple words that can be found in a dictionary. By using a brute force approach, 18% of your team's passwords can be guessed within 10 minutes. 90% of its passwords can be obtained within 48 hours. How is this possible? If a password contains a 4 digit number, there are $10 \times 10 \times 10 \times 10$ possible combinations (10,000 total). Ignoring Internet connection speeds, a good PC can manage 1,000,000 combinations per second.
- While password files are often the target, individual passwords can be obtained using tools that examine network data traffic.

Access to information is typically granted based upon something the user:

- Knows – Id and password
- Is – Biometric fingerprint, voice recognition, etc.
- Has – Access card, token, hardware device, etc.

Strong security systems use two of the three items listed above. For example, a strong security system could require both a password and fingerprint before granting access to information.

Your Team's Weak Points

Intruders know to look for the weakest link in the security chain. Often times the interaction of people to systems is a known vulnerability. Intruders use tactics such as:

- Dumpster diving. Intruders know to look at reports in the trash to identify account numbers, user ids, client names, etc.
- Intimidation. Intruders use intimidating tactics on the phone to get users to volunteer confidential information.
- Kindness. If intimidation does not work, intruders try and kill their targets with kindness. Users frequently try and go out of their way to help a friendly voice on the phone.
- Remote assistance. Many teams reduce costs by managing and maintaining IT systems from remote locations. Intruders know that administration of IT systems from remote locations increases the chance of compromising your team's information systems.

New Team Members

Intruders know that IT professionals install many hardware and software products right out of the box. Instead of testing the systems in a non-production environment, the equipment is left in its default state with every feature or service turned on. This provides the intruder an opportunity to access systems in a variety of different ways. Intruders know:

- Installations. Customers and hardware and software vendors all want a successful installation with very little configuration time. To make their products look good and to reduce installation problems, many products are shipped with all of their connectivity options "turned on". Turning on product features opens additional doors for intruders.



- Defaults. Many products are shipped with default ids, passwords, and access privileges. Intruders know to look for default configurations (e.g. administrator as the user id).
- Connectivity. Systems are initially configured for connectivity, not security. Intruders know that many hardware and software products have features that provide additional opportunities.
- Options. Intruders know that some equipment, like a firewall, starts secure when initially shipped from the factory. To get e-mail, Internet connectivity, and file downloads to function, IT professionals change the equipment configuration. Intruders know that by changing the equipment configuration of a secure product, the IT professional has created an additional opportunity to compromise the system.
- Testing. Intruders know that most IT professionals are overworked and understaffed. They install and configure systems but do not use external teams to audit their systems and procedures.

Five Steps to Intruding

Intruders typically take five steps to gain access to systems:

- Probe. Intruders often use scripts and tools to search for opportunities and vulnerabilities. One easy approach is to wait for a vulnerability to be announced then search for systems that have not applied the appropriate hardware or software patch⁹.
- Exploit. Once a vulnerable system has been identified, the intruder will exploit the opportunity to gain access to the system.
- Enhance. Often times, the intruder first gets access to a system with lower level access privileges. It then becomes a game for the intruder to find ways to get higher and higher privileges until he has full system administrator rights.
- Compromise. The intruder knows that having full system administrator rights is not sufficient. Once the intruder has the rights, he uses his access privileges to examine and potentially alter the system and its information. At this point, the information has been compromised and data integrity is in question¹⁰.
- Tracks. Once an intruder has compromised a system, he frequently covers his tracks to erase evidence. In this process, the intruder may erase log files, remove ids, stop backup systems, etc.

In addition, an intruder may install a backdoor or other tool that allows access to the compromised system. The backdoor may allow the intruder access to the information system even if the team changes the passwords on all of its accounts.

Game Plan

Many teams lack the staff, funding, and resources required to implement a formalized security solution. In the absence of a formalized solution, these teams implement point-solutions rather than enterprise wide security.



The game is complex with an enormous volume of hard to identify information. Teams should rely on experienced professionals to guide them through the complex balancing act of providing access to systems while keeping out intruders to successfully win the game.

References

1. Jupitermedia Corporation (July 2001).
2. Northwestern University Kellogg School of Management, Zell Center for Risk Research (2002).
3. Wall Street Journal (September 2000).
4. Up Side Magazine (February 2001).
5. AOL Digital Market Survey (2002).
6. Expert Magazine (June 2002).
7. Ibid.
8. Network Computing Magazine (2003).
9. CNN Chinese Hackers: No site is Safe (2008)
10. Altius IT Spyware, Kiss Privacy Good-bye (2008)

Publication and Author Information

Jim Kelton is Managing Principal of Altius IT (www.AltiusIT.com), an IT security audit, security consulting, and risk management company based in Costa Mesa, California. Mr. Kelton has over 30 years of experience in the Information Technology industry and is recognized as a security expert. He is certified by the Information Systems Audit and Control Association (ISACA) as:
Certified Information Systems Auditor (CISA)
Certified in Risk and Information Systems Controls (CRISC)
Certified in the Governance of Enterprise IT (CGEIT)

He sits on the Board of Directors of the following associations and organizations:

- Association of Professional Consultants (APC)
- International Association of Professional Security Consultants (IAPSC)
- Technology Professionals Association (TPA)