



White Paper
Intel Wargaming

Wargames: Serious Play that Tests Enterprise Security Assumptions

Tim Casey

Senior Information Security Analyst
Intel Corporation

Brian Willis

Senior Information Security Analyst
Intel Corporation

Executive Summary

Contents

Executive Summary	2
The Changing Face of Enterprise Attackers	3
Wargames: Collaborative Malevolence	3
How to Run a Wargame	4
Running the Game	6
Thank Management	7
Learning from Wargames	7
Conclusion	7

Most enterprises today have invested millions of dollars in securing their data centers, factories, offices, and other assets against security threats. Their risk assessment methodologies and security precautions are usually designed by a single group of people—internal information security specialists—and aimed at understanding vulnerabilities in a particular environment.

However, security threats come from living, breathing opponents who are creative, knowledgeable, collaborative, and determined. They also have a big advantage over the enterprise experts in thinking outside the box, because they are outside the box. To anticipate and better prepare themselves for attack, enterprises today need to move beyond understanding their environments to understanding their opponents.

To do a better job of this, Intel has embraced wargaming as an additional type of risk analysis that helps us better understand and defend against malicious attackers from within and without. Wargames are intense role-playing exercises that involve a multi-disciplinary cross-section of the organization, from facilities to finance, IT staff to factory worker. The goal is to move knowledgeable experts into an attacker role and pool collective knowledge and skills to pose a range of attack ideas. The results are very often surprising—and uncover new vulnerabilities that no single individual sees when viewing threats through the shuttered view of a single discipline or business area.

After several years of running wargames, Intel can offer a generalized blueprint as well as tips for making the efforts successful. Wargames are not a security cure-all and are not appropriate for every threat. They require a commitment from top management and participants, as the cost is borne by a number of groups besides the security group. However, wargames are worth the effort if an organization is serious about defending its most valuable assets against shape-shifting attackers who are smart, well funded, and dead serious about getting into your enterprise.

The Changing Face of Enterprise Attackers

Enterprise security is an arms race. There is no such thing as winning; rather, it's a matter of staying one step ahead of attackers. As attackers evolve and become more sophisticated, enterprises must follow suit.

The increasing and evolving sophistication of attackers is the chief threat that enterprises need to guard against today. In the last 10 years, the profile of the enterprise attacker has changed dramatically. The 17-year-old high school hacker out for a little mischievous fun is no longer a serious threat. Some of the most damaging attacks on businesses are from insiders—trusted employees or contractors—who are backed by organized crime, nation-states, and terrorist organizations after money, technology secrets, and political advantage.

These insiders are trying to crack employee databases to steal Social Security numbers to be sold to the highest bidder. They are after the secret recipes for microprocessors and other technologies that they can sell to nation-states or use for military advantage. They are after billions of dollars in electronic funds that can be surreptitiously siphoned into private accounts to fund terrorist activities. These attackers are well funded, have access to top minds all over the world and, because they're part of a global operation, are working around the clock to storm your gates.

Why aren't existing security tools sufficient against the new breed of attackers? The problem with traditional security tools and evaluations is that most are single-point, single-technique defenses. Attackers today are blending methods of attack and using many different techniques. For example, an insider may leak information about a delivery route to an outside accomplice, who will use that information to enter the facility and steal security credentials that someone else will use to hack into a company database. These scenarios can take on a James Bond kind of complexity and level of intrigue, but this is exactly what corporations are up against today.

Enterprises, too, need to learn to blend tools and techniques to keep pace. Understanding the nature and abilities of attackers is essential for effective security, but day-to-day job responsibilities typically confine internal staff members to the defender mindset. Traditional security defense literature tends to talk in terms of amorphous threats, viruses, malicious code, and other impersonal terms. But living, breathing, scheming people are the ultimate threat, and enterprises need to understand their motivations and techniques to defend against them.

The sheer pervasiveness of technology across a typical enterprise is another factor that makes today's security environment tougher than environments of 20 years ago. It is increasingly difficult for an enterprise IT department to control and protect all enterprise technology assets. Workers ranging from loading-dock personnel to salespeople use business-critical applications and technology around the clock, outside the enterprise walls. The IT group may not have a clear view of how these technologies are being used or where they are after they've been issued. A salesperson may add vulnerable applications or peripheral devices to his company-issued smartphone or notebook computer. A computer in a remote warehouse may be left unattended for long stretches during the workday even though it's supposed to be behind locked doors.

With the growing ubiquity and complexity of the enterprise computing environment, it is very difficult to predict the unintended consequences of far-flung technology deployment. An enterprise grows organically and exponentially, and technology usage far beyond the data center or even the desktop means that enterprises can no longer leave risk assessment to a few IT personnel working behind closed doors at headquarters. More players need to be brought to the table—factory workers, salespeople, facilities personnel, finance people—to bring new perspectives and sleuth out new vulnerabilities together.

Wargames: Collaborative Malevolence

Like many multinational companies, Intel is an attractive target for this new generation of high-tech thieves. Intel spends billions of dollars each year on research and development of leading-edge microprocessor technology. Many of our research areas are of keen interest to competitors and nation-states that are hunting for high-tech secrets. We naturally want to protect our investment and our future.

To this end, the Intel Information Risk and Security Group began using wargaming several years ago as a unique new risk assessment methodology. Although wargaming is common in the military and as old as war itself, it is relatively new to enterprise IT. Wargames are intensely focused exercises in which a multidisciplinary set of experts gets together to focus intense scrutiny on assets from an attacker's point of view. By rigorously testing our security assumptions, we are able to uncover vulnerabilities that just don't surface when using traditional risk assessment techniques.

White Paper Intel Wargaming

Let us emphasize that we are speaking of tabletop wargaming, not staging actual attacks on production systems and networks or even clones of these systems. Wargamers gather in a room, around a table, with nothing more than one or two notebook computers that they use to look up ideas on the Internet. Staging mock attacks on production systems is far more expensive than tabletop wargaming and is not a realistic option for most companies, though Intel continues to investigate safe ways to deepen the realism.

Wargames help enterprise professionals better understand attackers by temporarily becoming attackers. These games are characterized by a) understanding and emulating a specific attacker mindset, and b) taking a multidisciplinary approach to enterprise defense. While traditional defense tests are conceived and run by the IT or security staff, wargames pull in knowledgeable people—beyond the security experts—from across the company. Wargames focus the attention of multiple experts on a specific attack goal, exploiting multiple vulnerabilities in unique and often unforeseen ways.

On the surface, wargaming sounds a lot like penetration testing, in which a small group of experts, sometimes from an outside firm, attempts to penetrate your defenses. However, penetration testing does not always involve a multidisciplinary approach nor does it include anyone outside this small group of security professionals. Similarly, an audit is an exercise in getting through a checklist of best-known methods and controls. But in an audit, auditors stay in their defender mindset.

In a wargame, you gather many diverse people from across your company in one room and turn them into bad guys. This diverse group might include business process people, salespeople, logistics people, facilities people, and others who would not typically sit at a table together. When these people from across your organization begin to collaborate and pool their expertise with the goal of protecting your company, and stay at it for a couple of days, some surprising attack vectors emerge that security professionals working alone might never see.

How to Run a Wargame

The Intel IT Information Risk and Security Group has devised a wargame methodology that includes intensive training for security professionals in advanced offensive threat design and a detailed set of attack scenarios against particular assets. We have staged wargames to better understand threats to a broad range of Intel assets including factory operations and our supply chain.

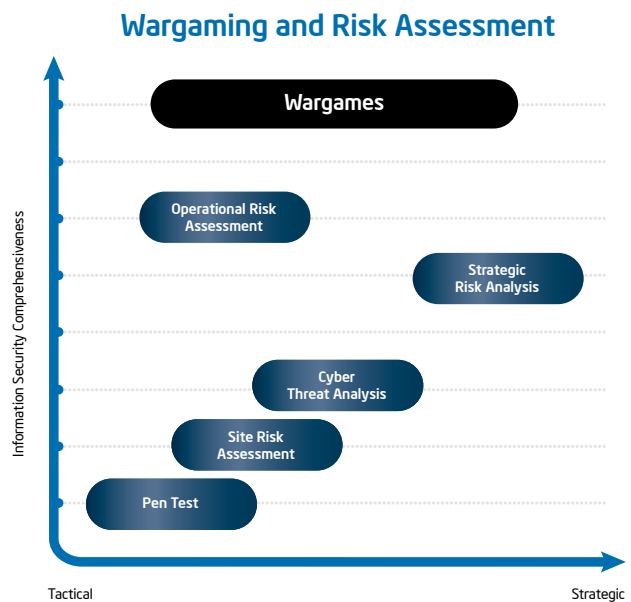
In designing a wargame, the Intel Information Risk and Security Group recommends assessing the value of a wargame investment for a particular business area, evaluating the existing security environment, then systematically executing the steps involved in designing and running the game.

To Game or Not to Game?

First, you must ascertain the nature and value of the assets being protected. The asset might be a factory, a network, or a shipping lane. Your key rule of thumb is not to spend more on security measures than the asset is worth. Penetration tests or some other type of security analysis might well be better suited for targeted assets such as a product launch or an inter-company connection or business application. Because wargames require a large number of people and a significant amount of time—one to three days—make certain that your internal client is prepared to make the needed resource commitment.

Wargames are better suited to handle broad questions such as: What are the risks of setting up an offshore development office in a particular country? What would it take to disrupt a supply chain? Could a single outsider seriously disrupt a factory or would it require inside help?

You should also consider a wargame if you need to convey information to management in a meaningful way. Penetration test results can often be a dry list of facts and figures that are difficult to translate into a reason for action. Many managers are not security experts, so wargames can establish a common language that allows the security experts to explain complex and often esoteric risks in a way that makes the risks' impact immediately relevant to everyone.



Assess the Existing Security Environment

Once you have determined that a wargame is an appropriate and affordable measure for the asset or scenario in question, assess the existing security environment surrounding that asset. Which employees are involved? Are they highly monitored, trustworthy employees that have been employed for 10 years or a parade of short-timers that turn over frequently? Which external people, such as vendors, are involved? What kind of mitigating controls are already established, such as cameras, guards, and traffic logs?

With answers to these kinds of questions in hand, talk with internal security experts and come up with a rough idea of the kinds of scenarios that would realistically apply in this situation. You might pose a disgruntled-employee scenario, a vendor-assisted scenario, or others. Share possible scenarios with your client and have them validate those that they think are possibilities and eliminate others that they think they have covered.

Design the Wargame

Planning is critical to a successful wargame. Based on what you have learned from conversations with your internal client and your own observations, define the specific scenario being “gamed,” decide which employees to invite as participants, and explain to participants how the game will work. You also need to assign a facilitator and a scribe, determine how long the game will be, and decide where it will be.

Define the scenario(s). In conjunction with the client and subject-matter experts, the wargame team develops and refines the scenario(s) to be tested. If possible, create at least two scenarios, a “most likely” and a “most damaging.” Intel also commonly creates one or two additional scenarios than we think we will need, in case one primary scenario does not fill the time allotted for the game.

Here is an example of a specific wargame scenario that Intel might pose:

A disgruntled factory worker is angry about his last performance review and wants to get back at the company. He also wants to keep his job so doesn't want to get caught. He thinks some sort of wireless attack on the factory is his best option, because wireless is remote and doesn't leave fingerprints. He has a good knowledge of the factory, can follow directions for simple attack tools found on Web sites, but he is not a networking or wireless protocol expert. He is willing to spend up to \$400 to carry out the attack.

Note the degree of specificity in profiling the attacker and his goals. Be as specific as possible in defining the game scenario so that it seems real. First, define the attacker. The Intel Information Risk and Security Group has created attacker archetypes, similar to personas used in systems analysis work, to better understand attacker mentalities. These archetypes, recorded in the Threat Agent Library [available at <http://communities.intel.com/openport/docs/DOC-1151>], include disgruntled employee, opportunistic employee, industrial spy, politically-motivated attacker, and others. Specify the skill levels of the attacker(s) in the scenarios, the amount of money they are prepared to spend, the kind of attack they want to accomplish, and their timeframe for both planning and execution.

Remember that you are writing a story premise that needs to be compelling, realistic, and engaging for the people acting it out. At the same time, you are not writing a script; do not detail the action so completely that the outcome is predetermined. Also keep in mind that the audience members may not be security professionals and come from a range of areas within the organization.

Invite participants. The next step is to determine which individuals to invite as participants. Look for a good mix of people who can cover the relevant areas described in the scenario—in the example given above, look for individuals who know a range of details surrounding the factory being attacked. In our example, you would look for someone who knows the physical layout of the building, someone who knows the consequences of crippling various machines, and someone who knows what it takes to return these machines to operation and how long repairs would take. Because the employee in our example is considering a wireless attack, you would also include a wireless expert.

The group you gather does not have to represent every possible twist and turn in the scenario; there is no way to know in advance of the game what those twists and turns might be. You can always follow up with additional experts if new vulnerabilities are identified during the game. Real-life attackers will not have all the answers, either.

We have discovered that too many people together can reduce the effectiveness of a wargame. In keeping with the general principles of team dynamics, too many participants can cause the group to break into sub-groups and multiple conversations. We have found that a group of 8 to 9 is optimal, with 10 to 12 maximum. For a very complicated wargame, or one that spans many sites or geographies, you can set up multiple cells and define the rules by which cells can interact. Each cell might contain a mix

White Paper Intel Wargaming

of experts, or you may group the cells by subject, e.g., a Finance cell, an IT cell, and so forth. Members of the same cell must be located in the same room, although cell-to-cell interaction may be virtual.

Assign a facilitator and a scribe. Two key roles need to be assigned beforehand. A facilitator, usually a member of the information security team, has the assignment of guiding the brainstorming session. This individual keeps the game focused on the specific scenario, arbitrates, sets time limits, involves all participants, and keeps the conversation going until the group has run out of ideas on a particular topic.

A scribe is the other assigned role. This individual is not a gamer; their only job is to take comprehensive notes as ideas are offered and discussed and the game is played out. We have found that even experienced gamers cannot participate and take adequate notes at the same time. You must have one scribe per cell, physically located in the room with the gamers.

Explain the ground rules. Wargame participants need to be relieved of all responsibilities during the game and to understand that they have made a commitment to providing inputs during the session. However, they are not responsible for formulating responses.

Participants also need to understand that they are not to use their cell phones or to send, review, or respond to e-mail messages during the game. In fact, notebook computers are allowed in the room only for the scribe and for looking up information on the Internet in the role of an attacker. For example, attackers might wonder if they could find a map of a particular building online; they need to be able to find out during the game.

Choose the site. It's best to get off campus for a wargame, though moving to a hotel presents security concerns and can make it difficult to adopt a diabolical mindset. You do not want non-participants to have access to the meeting room. Intel typically holds wargames at a different Intel campus to get away from the gamer's everyday environment. Regardless of the setting, players must attend in person and away from their desks. You should at least have a large conference room, one that accommodates twice the number of individuals that are gaming.

Whatever the site, it's important to treat the gamers as honored guests. How you do this depends on your corporate culture. Intel gamers always receive a reward (such as a gift certificate),

a commendation copied to their manager and, if possible, a small playful memento such as a toy secret decoder ring. Food, of course, is a necessity. It's best to cater lunch to minimize people leaving the room.

Intel typically holds a one-hour preparatory session for participants before game day to explain what they are heading into, lay out the rules, and maybe even preview the scenario(s). Explain the wargame techniques, the need for commitment, and the need for the utmost confidentiality

Running the Game

Very often, once inside the room, participants don't "get it" right away. Either they have been in a defender mindset for so long that they don't understand how to think like an attacker, or they are not used to thinking about security issues at all in their daily responsibilities. For example, gamers may initially assume a particular area is safe because it is covered by security cameras and therefore consider the scenario "not possible." The attacker, however, sees that as a puzzle and will first plan how to circumvent the cameras. It's the facilitator's job to continually bring participants back to the goal of the game and the objectives. It can take one or two hours for even experienced gamers to cross over to an attacker mindset. This is why it is essential to stage wargames for a minimum of six to eight hours.

Some participants are also uncomfortable in plotting to harm their coworkers or company, especially in areas where violence is common. To help the gamers feel comfortable easing into the attacker mindset, we try to start the game with a scenario that is simple and non-threatening.

Once participants do make the transition to the "dark side," you often need to reel them back in. They will come up with ideas that are outside of the engagement condition ("Let's kidnap the company president!"), focus on low-probability scenarios, or venture outside the scope of the scenario conditions (such as forgetting that the attacker only has \$400 to spend). This is why the facilitator is so important; he needs to allow a certain amount of free reign while keeping participants within the game parameters. Sometimes, however, if a participant keeps coming back to a far-fetched scenario, you should take a few minutes to explore the idea. The individual may have uncovered a real potential danger but just cannot articulate it realistically themselves.

Be prepared for surprises. This is the whole value of a wargame. Because of the interdisciplinary makeup of the team, you will hear both grass-roots and big-picture perspectives that may well uncover just how easy it is to cripple a key asset. For example, in one wargame aimed at disabling a manufacturing production line, several participants focused on taking out various servers or other expensive or hard-to-reach assets. A factory worker recommended simply disabling the printer used to print shipping labels. This simple action had exactly the same effect as more complex suggestions at a much smaller cost.

Document everything. In a wargame, you usually do not know what you have gathered until well after the game. The scribe needs to write down every suggestion, including who provided each comment, and how the team used the ideas offered. Because it's impossible to go back and capture comments once the game is over, it's vital to capture everything that happens for the purpose of the post-game analysis.

Set time limits. Wargames can run from six hours to three days, but do not play longer than three days; it becomes too intense. Day-and-a-half games work well, giving participants the chance to go home, think about the game, get a good night's sleep, and come back the next day with new ideas.

Thank Management

Participants' managers will not be privy to the details of the wargames, because it is a classified activity. They may not see a direct payback for their employees' time. Send a message of thanks to managers emphasizing that their employees were valued contributors to a confidential project of the utmost importance to the enterprise.

Learning from Wargames

Intel has not created a model or template for distilling wargame findings. Just as in other types of risk analysis, poring over the scribe's notes and understanding the story that emerges is more an art than a science. Remember, though, that a wargame is just another means of gathering information, another tool in your arsenal of risk assessment methods.

When the wargame is over, an analyst will use traditional techniques to analyze the game data and convert the data to recommendations. The analysis will yield a detailed course of action for addressing vulnerabilities discovered. These recommendations and actions can be entered into a risk management tool to track their completion.

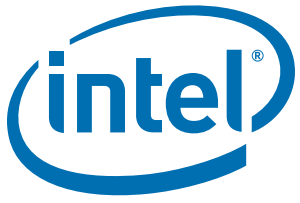
In post-game analysis, the analysts will often uncover discrepancies between the internal client's initial statements about the asset versus your discoveries during the games—for example, procedures they thought factory workers followed versus what they actually do. Key learnings often incorporate not only vulnerabilities but identification of what is important to workers in that environment.

Sometimes, you will learn from a wargame that your internal client does not have a security problem after all. However, wargames usually do uncover risks. The analysis team may develop detailed recommendations for mitigation measures or simply present the risks discovered with suggestions for the kinds of precautions the client might consider, as previously agreed upon by the client and wargaming team.

Conclusion

In conclusion, there is no silver bullet in corporate risk assessment. Wargaming is a new tool, along with penetration tests, site assessments, and others, that enterprises can use to look at broad risks in a way that traditional security analysis tools do not allow. Wargaming provides the following benefits:

- Wargames let organizations rigorously test their security assumptions and find hidden vulnerabilities.
- Wargames provide great hands-on training opportunities for security and non-security professionals involved.
- Wargames bring security professionals and business people together in a positive environment to strengthen enterprise security.
- Wargames provide actionable information about real-world vulnerabilities and threats.
- Wargames make security threats real to rank-and-file employee in a way that posters and other cautionary measures cannot.



www.intel.com