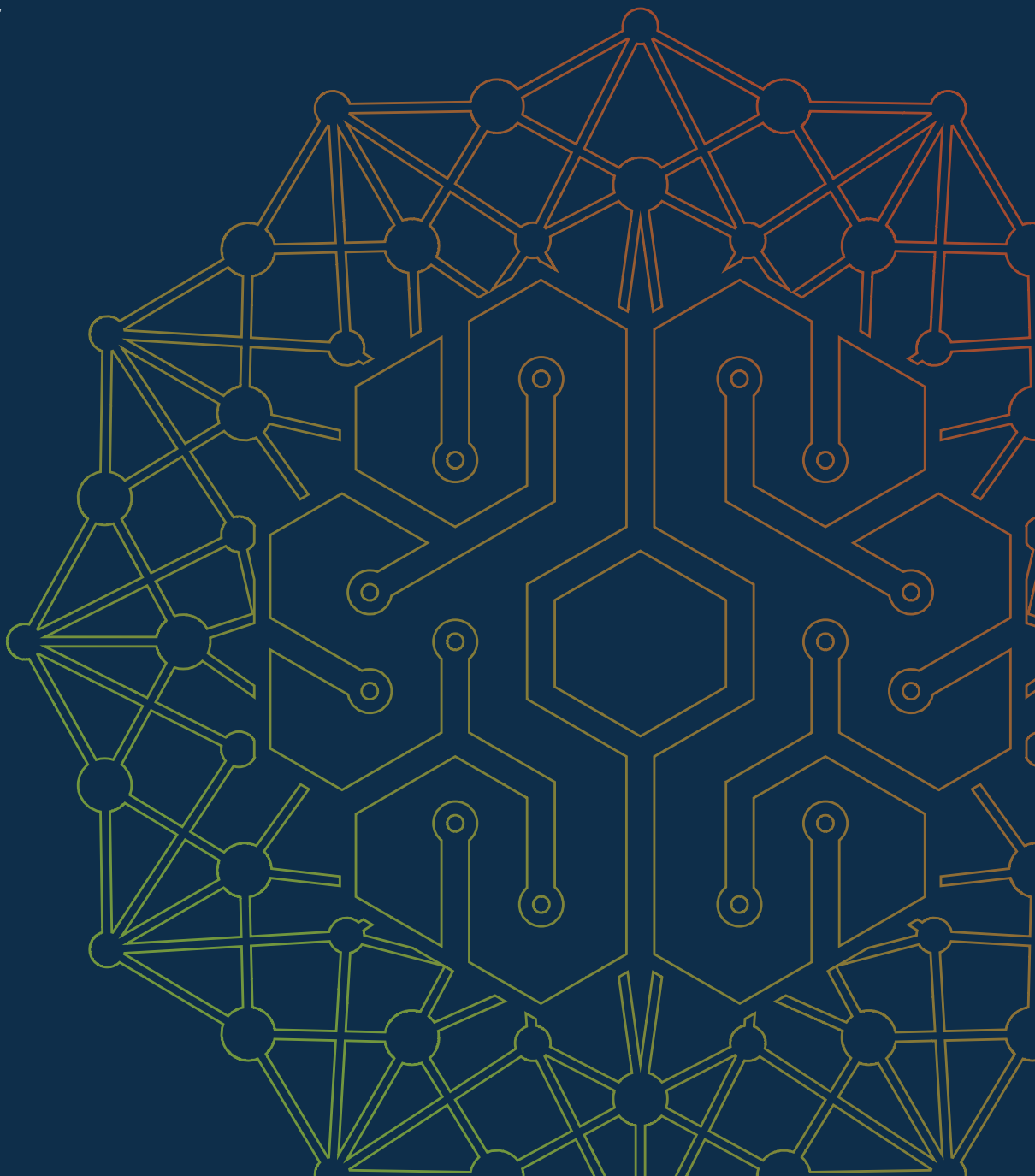
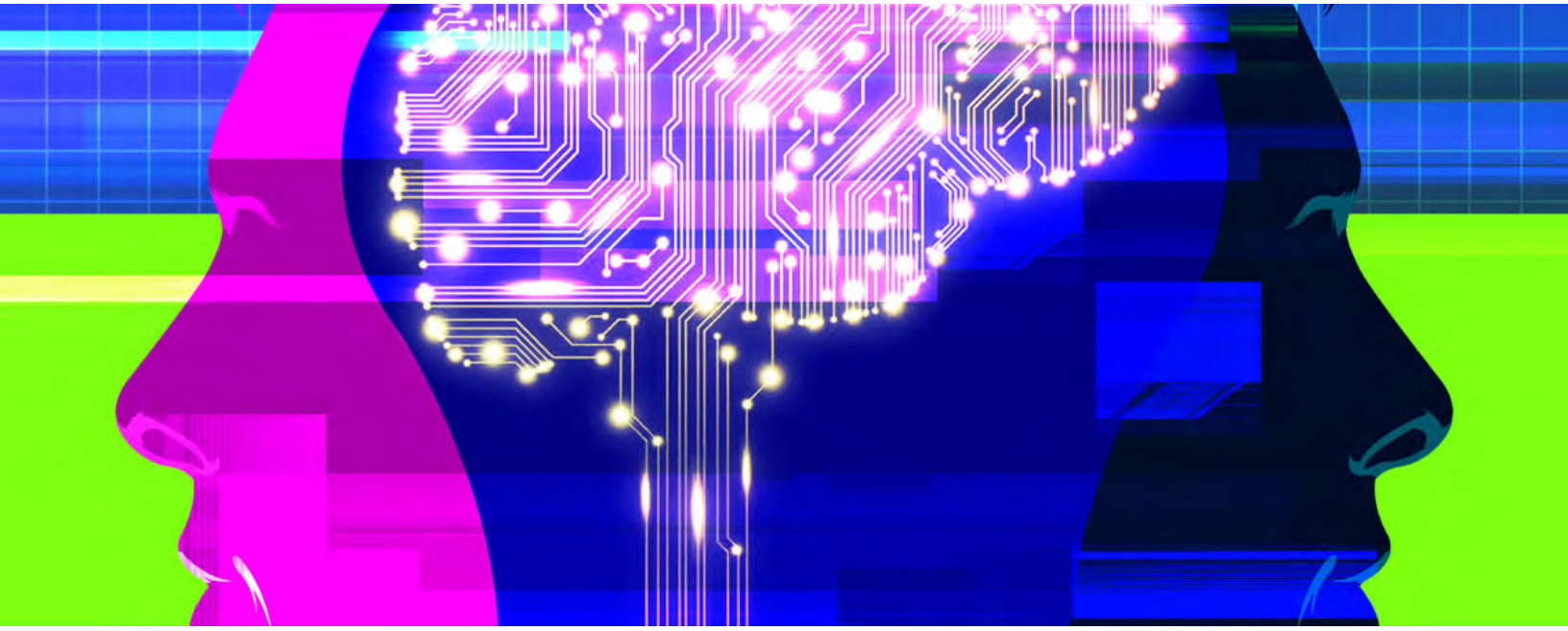
ASIS INTERNATIONAL
Advancing Security Worldwide®

How to Use the **ATTACKER MENTALITY** for Good

By Val LeTellier



Through focus, patience, and non-linear thinking, malicious actors create new paths into organizations. Defenders can use attackers' tactics against them.



Society would be far less enjoyable if we all adopted an attacker mentality. Everyone's first thought upon meeting someone new would be how to manipulate them for personal gain. Each encounter would be based upon the assumption that there are no rules of engagement, political correctness, manners, morality, or conscience at play.

Attackers are comfortable doing things that most people aren't. They look for exploitable motivations and vulnerabilities to create self-serving situations. They are comfortable masquerading as someone else, building false relationships, and hiding the truth. For instance, attackers have no qualms about following your CFO home to collect personal information, booking a room on your CEO's hotel floor and "getting to know" him or her at the hotel bar to collect details about the company, sending your IT staff

cool gifts laced with malware, or even using Facebook to send your kids a malicious link hidden within a game.

These guys are different. They take it up notch or five. But what, exactly, sets them apart?

Singular mission focus. Professional attackers are not distracted by what is happening on the sidelines; they focus exclusively on mission achievement. They are not constrained by administration, bureaucracy, or budget, and they do not make decisions by committee. They know what they want, and they go for it.

If you ever wanted to know the comprehensive list of valuables you have access to, just ask an attacker. They will know because they are always sizing up people and opportunities for personal gain.

You may be surprised by what attackers consider valuable and why. It may sometimes be as obvious as money or intellectual property, or it could also be other items. In today's world, opportunities for financial gain are much broader than before. Attackers may seek different items, depending on whether they are thieves, conspirators, leakers, discontents, or opportunists. One's reputation, relations, personnel, speed of business, and mental wellness can be targets for specific attackers with specific agendas.

Using data as an example, the cybersecurity "CIA Triad" of confidentiality, integrity, and availability tells you that theft is not the only threat—an attacker could also harm your organization by clandestinely disrupting your data integrity or denying you or your customers access to your data.

Patience. Ever found yourself in the right place at the right time? Whether we attribute it to luck or serendipity, most of us also seek to create those situations for ourselves in our daily personal and professional lives, but our results are usually hit or miss. We simply can't be in all the

right places just waiting for the right time to come around. But that is exactly what an attacker does.

In the cybersecurity world, digital "honey pot" websites allow attackers to lie in wait for unsuspecting victims to come to them. In the physical world, attackers tailgate by loitering near a door to a facility and following someone with legitimate access into the building.

Their greatest advantage is your greatest challenge: the attacker only needs to be right once, but defenders must be right all the time.

Nonlinear thinking. While most people see a direct line between points A and B, attackers often look at how points D and F can get them to point B. They see patterns and then figure out when those patterns stop applying. They find the edge between "yes" and "no" and test how sharp that edge really is. They ask open-ended questions, begin with more than one premise, make deductions, and then infer ways forward. If that path is blocked, they repeat the process from the beginning. Attackers seeking weaknesses in software exploits often follow this process; the program is viewed holistically, leading to specific premises, deductions, and inferences that point to security gaps.

Defenders face the immense challenge of shutting down paths they can't conceive of in the first place.

This linear thinking is applied within each phase of their attack: performing reconnaissance, scanning and enumerating, gaining access, escalating privilege, creating redundant access, and covering their tracks.

Attackers look at problems without blinders. They see the complete picture and never rule out an implausible

option if it could help them achieve their goal. Defenders face the immense challenge of shutting down paths they can't conceive of in the first place.

Backward reasoning. Attackers visualize their goal and work backward, which allows them to identify all possible accesses and paths, especially ones unidentified and unprotected by defenders.

Known by various terms (backward chaining, reverse engineering, purposeful task analysis, retrograde analysis, or backward induction), backward reasoning is a well-recognized methodology. Before Amazon designers and developers start a new project, they write a hypothetical press release from the future, celebrating the success of a product. From there, they determine what needs to be done to get to that point of success. And it is the second of Stephen Covey's *Seven Habits of Highly Effective People,* "Begin with the end in mind."

In 2006, retail giant TJX Companies Inc. (TJX), experienced two notable examples of attackers working backward from the company's lucrative customer record data. Attackers used in-store job application computer kiosks to deploy malware through mouse/printer USB ports, turning the devices into remote terminals with access to the main network. The firewalls on TJX's main network weren't set to defend against malicious traffic coming from the kiosks. Months later, attackers accessed an improperly secured Wi-Fi network from the parking lot of a Marshall's store in St. Paul, Minnesota, and exploited the deficiencies of the aging Wired Equivalent Privacy (WEP) wireless security protocol. More than 45 million records of customer payment data and untold revenue were lost.

By any means necessary. Although attackers maintain a single-mindedness in their focus, this does not mean they limit themselves to a single vector or approach. They

use whatever works, whether it is within the virtual, human, or physical domains. What the average defender defines as "all possible attack vectors" is almost laughable to someone who has no rules.

THE ATTACKER MENTALITY AT WORK

The attacker mindset and approach were showcased in an attack against a major oil company in 2014. Unable to breach the company's computer network, attackers instead injected malware into the online menu of a Chinese restaurant popular with employees. When workers browsed the menu, some were socially engineered into unknowingly downloading code that provided the attackers a narrow foothold in the company's network. From there, the attackers found an opening to create a company identification badge that allowed them to pose as an IT vendor and get physical access to the firm's servers.

This operation demonstrated attackers' ability to exploit vulnerabilities across their operating environment, specifically within the digital, physical, and human domains. Understanding the interconnectivity and interdependency of these domains and the aggregated risk they pose is a critical first step in the development of an organization's risk mitigation strategy.

The virtual attack surface. The escalating amount of attention that the virtual domain receives is merited. Risk within the digital domain is already extremely broad and exponentially growing, ranging from a lack of operational security to bad policies to bad code to executives' insecure home networks.

In the rush to launch competitive products and the prioritization of user convenience over security, manufacturers have often neglected necessary security safeguards. And thanks to our reliance on the Internet, attackers can

now compromise almost anything—surveillance cameras, access control systems, microphones and cameras on smartphones and laptops, thermostats, vehicles, and industrial control systems.

The danger of combining an attacker mindset and widespread connectivity was exemplified in an attack against a North American casino in 2017. Using an Internet-enabled fish tank, attackers exploited sensors connected to a facility PC that regulated the tank's temperature, food, and cleanliness. As a result, 10 GB of private data was sent out to a device in Finland.

Using social engineering, attackers exploit human nature.

The security industry is most focused on the virtual attack surface, often developing automated digital countermeasures to identify a "silver bullet" solution. This approach addresses only part of the risk equation, and the effectiveness of each solution is reliant upon the diligence of those operating or engaging with the system. In the end, human behavior can either reinforce or degrade security measures.

The human attack surface. Employees, trusted vendors, and partners represent potential weak links. Using social engineering, attackers exploit human nature to access facilities, networks, and valued items. They can create well-researched and believable ploys to get what they need, incorporating techniques like pretexting, baiting, and quid pro quo.

Social engineering is a serious discipline with serious consequences. At DefCon's annual Social Engineering Capture the Flag event, the security practices and counter-

measures of many top firms have been compromised by a talented attacker armed with just a phone.

A great example of social engineering is a 2007 attack on Antwerp's ABN Amro Bank. No one knows his real name, but the staff knew him as Carlos Hector Flomenbaum. He billed himself as a successful businessman, and he had frequented the bank for at least a year. The bank's employees loved Flomenbaum. He brought them chocolates, talked to them about non-diamond-related matters, and ultimately won their trust to the extent that he was given VIP access to the vault. One night in March 2007, he let himself in, broke into safety deposit boxes, and walked out the front door with $28 million in diamonds. The bank had a $2 million security system. Flomenbaum has yet to be caught.

The physical attack surface. If an attacker can gain access to the premises, he or she can quickly access sensitive information—both through the network and in hard copy. Inadequate physical security controls can render most technical controls useless. Interestingly, while firms traditionally expended most of their resources for physical security, it is now far subordinate to digital defense. And this change would be more dramatic if it weren't for the increasing attention paid to workplace violence.

To penetrate physical defenses, attackers collect data via open sources and create sophisticated approaches that manipulate access control though social engineering, badge cloning, and close network access.

A well-used attack plan is the select placement of USB sticks labeled "payroll," "sensitive," or "personal" with embedded malware ostensibly dropped in public areas around a company. Well-meaning or curious employees will launch the attack themselves by connecting the USB to a work computer.

Across all attack surfaces, the attacker mentality is characterized by function over form, exploitation of simple vulnerabilities, being noisy or quiet depending on operational need, aggregating bits of seemingly meaningless data, utilizing unwitting or complicit surrogates, employing patience and gradual privilege escalation, creating backup access channels, and utilizing burnable channels to erase one's tracks.

USING THE ATTACKER MENTALITY FOR GOOD

The proper application of the attacker mentality can prevent an insider attack; protect the organization's most valuable resources, up-time, reputation, and jobs; and save security professionals from embarrassment and loss of stature.

But more specifically, the attacker mentality allows you to have insights normally unavailable in a risk assessment. It reveals a more comprehensive list of valuables, not just what matters to you, but also what others may covet; it identifies an attacker's most lucrative vectors; and it reveals attack vectors that can exist in places you've never imagined, such as partners, vendors, suppliers, insurance providers, HVAC equipment, printers, thermostats, videoconferencing software, vending machines, and fish tanks.

The bottom line is this: analyzing your organization using an attacker mentality allows you to identify the security gaps most likely to be used against you. Identifying those gaps and quantifying the associated risks are critical to obtaining stakeholder support and funding for insider threat programs and exercises.

Consider that famous Mike Tyson quote, "Everyone has a plan until they get punched in the mouth." An insider

Start with the conviction that your security systems have exploitable gaps.

attack is like a punch in the mouth. Your conventional wisdom—your plan—takes a hit, and the world stops spinning for a second. You wonder where you are, what weakness the attacker exploited, what gaps you need to close, and which of your strengths you can rely upon to survive.

By leveraging the attacker mentality, you can have the all the knowledge that comes from a punch in the mouth, but without the broken jaw. To apply the attacker mentality to an insider threat program, first acknowledge that the status quo won't work. You have to accept that if you don't make some changes, the organization will be facing significant harm.

Second, change your own mentality. You cannot create effective insider defenses, risk management strategies, tabletop simulations, and security strategies if you are unsure how vicious, visionary, and committed your insider attackers are.

For many folks, the simple truth is that they are working against an enemy who is operating with a level of sophistication and determination they don't understand. Change your vocabulary, perspective, and approach. Stop sugar-coating attacks by using terms like "insider," "hacker," or "breach." Instead, use the terms "perpetrators" and "attack." There is a world of difference between saying you were "robbed" and "attacked," and the same difference exists between being "hacked" and "attacked." Train yourself and anyone with network access to acknowledge that the world has changed. The new reality is that everyone must practice the same common sense security at work as they do in public places: beware of strangers approaching with unusual requests, seeking quick and unconventional actions, and applying pressure tactics. If even for just a second, question whether the request, embedded link, or attachment makes sense. And if your gut check reflects any concern, pay attention.

Create environments that foster reality. Don't say "if it happens to us," "what are the chances," or "that is too far-fetched." Realize that there are two types of organizations—those that know they have been attacked and those that don't.

Practice symmetrical thinking. Think like your attacker; holistically examine and map out your strengths and weaknesses. Employ patience, nonlinear processes, and any means necessary in your reconnaissance and attack modeling. And start with the conviction that your security systems have exploitable gaps, that some of the

people you trust with privileged access will fail to do the right thing at the right moment, that you have items of value that you're not protecting. For many businesspeople, this is just not possible. Many are incapable of stepping into an attacker's frame of mind; therefore, it makes sense to hire attack experts or "red teamers" to provide that perspective.

Red teaming is focused on stopping the cut, not stopping the bleeding.

Red teaming is the practice of viewing problems from an adversary or competitor's perspective, a simulated attack that prepares you for the real thing. The goal of most red teams is to enhance decision making by challenging assumptions, identifying the adversary's preferences and strategies, and acting as a devil's advocate.

Just as an attacker will use cyber, physical, and social engineering to find the most effective way to breach your defenses, so will red teams. If your red teams have firsthand experience attacking hardened facilities and workforces, the results of a red teaming exercise and a standard risk assessment will be even more pronounced.

Red teaming is focused on stopping the cut, not stopping the bleeding. It can help assess your countermeasures, prepare you for a real attack, and test your incident response measures before an incident occurs. It is the most effective test of your insider resiliency.

Therefore, the best time for a red teaming exercise is before your organization "goes live" to the public or its members, and the worst time is after an attack. If your organization or new product is already "live," the second-best time to red team is after a security review and/or enhance-

ment. This allows you to test for any new vulnerabilities inadvertently created during the upgrade.

Red team testing can address both the inside and outside attacker perspectives, benign or malicious insiders, and actors that are being manipulated, guided, and protected by organized crime groups or intelligence services.

This testing will show you how attackers collect and analyze target data from personal observation, online research, and technical, physical, and human social engineering. It will demonstrate the privileged internal information and access that a determined attacker can realize in a short time with only moderate effort.

Effective red teaming will identify the security vulnerabilities that attackers would likely exploit first in an attack. There should be no off-limits areas for the red team, because real attackers will use any means necessary to breach your technology, people, and facilities to access your critical resources. Your technology includes networks, applications, routers, switches, appliances, and devices. Your people include your staff, independent contractors, business partners, and anyone with trusted access. Your physical infrastructure includes your offices, warehouses, substations, data centers, and buildings.

Operating from the viewpoint of your adversary, members of a red team will collect public data on your organization and key officials. Using that information, they will evaluate potential vectors for attack and determine the best attack plan. They will launch a blended attack involving several facets of social engineering, physical penetration testing, application penetration testing, and network penetration testing. Then they will capture and report details on your response to the attacks and recommend mitigation solutions to close your security gaps.

The key to maximizing the effectiveness of your red-team-

ing effort is selecting a team with a strong attacker mentality, cutting-edge technical penetration and social engineering skills, and a strong track record of working against hardened facilities, networks, and workforces. Then give them as much freedom of access, time, scope, and methodology as you can.

Insider risk represents an existential threat to your organization's survival. Using privileged access and situational awareness, a single insider can cause immense financial loss, reputational harm, and even layoffs and bankruptcy. Your organization's future depends upon stopping their attacks.

To stop insiders, you need to know what an attacker would want from your firm, who has access to those resources, and how an attacker would steal, alter, or deny access to them. Red teaming shows how real attackers will act, not merely how defenders imagine they will act.

That said, red teaming is not for the faint of heart. It often identifies weaknesses that you never knew you had and exploitable vulnerabilities that must be immediately closed. It provides a robust test of your incident response measures. It often is an eye-opening and sometimes embarrassing exercise for corporate security teams. But in the end, it is the preferred methodology for firms determined to do everything possible to secure themselves from insider attacks.

VAL LETELLIER HAS THREE DECADES OF RISK MANAGEMENT EXPERIENCE IN THE PUBLIC AND PRIVATE SECTOR. HE IS THE CHAIR OF INSIDER THREAT WORKING GROUP OF THE ASIS DEFENSE & INTELLIGENCE COUNCIL AND A MEMBER OF THE INSA INSIDER THREAT SUBCOMMITTEE.

SECURITY
MANAGEMENT

Learn more about Information Asset Protection.

To join ASIS International and become a subscriber to *Security Management*, visit *asisonline.org/membership/join*.

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals. *Security Management* is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.