FEBRUARY 2019

PRIORITIZING AND PROTECTING AGAINST THREATS FROM TERRORISM, CYBERATTACKS AND INSIDERS

SHULMAN ROGERS

PRIORITIZING AND PROTECTING AGAINST THREATS

*By Mark J. Maier**

Businesses face growing terror, cyber and insider threats on many fronts, but they are hamstrung by limited budgets that make choosing how and when to defend themselves more and more difficult. This rising cluster of threats demands substantial financial resources to protect people and assets. Recent domestic attacks in Pittsburg, Parkland, Orlando, San Bernardino and more show a disturbing speed of self-radicalization necessitating even more intensive security.

Companies facing these threats, however, have to live within limited budgets and make difficult choices, such as when to go beyond the legal minimum to effectively protect a brand. Making the right choices to minimize liability is even more important in the homeland, where private parties own the majority of assets and critical infrastructure and consequently have to deal with the results of a terror, cyber or insider attack. Relying exclusively on government organizations is not enough, since their activities are often classified, restricted or government-focused. Government shutdowns further restrict the ability for the private sector to obtain protection from the government.

Thus, commercial businesses themselves need to take the lead in addressing threats to their specific core missions and assets. Certain countermeasures need to be employed concurrently, while others can be implemented sequentially. Legal, operational and technical expertise should be engaged to analyze these risks, prioritize threats and implement mitigation measures. Negotiate applicable contract changes, ensure for regulatory compliance and enforce your rights when needed.

But how much security is required to meet the minimum legal standard of care for each of these different threats? In what situations must certain security measures be enacted to comply with a statute or avoid contractual breach? How much more security is needed to protect your brand?

To answer these questions, businesses must take the lead in addressing threats to their own specific assets using some countermeasures concurrently while implementing others sequentially. Not everything can be done at the same time. The three-pronged approach of separating threats, prioritizing them and customizing countermeasures can help organizations deploy their resources.

1. ***Identify and Separate Threats***: Characterize the group threats based on the attacker, weapon and intended target. Understanding the motivation for and intended target of an attack often matters more than the method in accurately assessing a threat.
2. ***Prioritize Threats***: Assessing threats by the types of attacks, severity of harms, liabilities and likelihood is vital to allocating resources.
3. ***Customize Countermeasures***: One size definitely will not fit all. Just as threats and damages are different, so are effective responses to them. Organization-specific assets driving the selection of countermeasures are provided, along with next steps such as negotiating proper contract terms and implementing regulatory compliance programs.

This article is intended to assist in an overall strategy on how to defend against numerous simultaneous physical and electronic threats. It is not a replacement for NIST, NERC, NISPOM or any of the various other specific security standards which should be followed. Also, this article discusses important national and homeland security topics which currently dominate the news with the understanding that there are many other threats, hybrids and topics which can supplement or revise these comments. Similarly, this article defines and uses key terms such as “terror” and “cyber” in certain ways, also with the understanding that they do not have single agreed upon definitions.

STEP 1: IDENTIFY AND SEPARATE THREATS

The first prong requires companies to focus on attackers' primary targets and motivations to determine the type of threat before looking at the weapons attackers might use. For example, terror threats target civilians for political or religious motives, while cyber threats target unaffiliated intangible assets such as finances, intellectual property or trade secrets. Identifying targets and separating motives allows for the following generalized categorization of threats as further described below:

Targets	Motivation	Type Threat
Civilians	Political, religious, etc.	Terror
Unaffiliated information, systems or assets	Theft, harm, exposure, etc.	Cyber
Co-workers or company property	Extortion, revenge, theft, etc.	Insider

Where attackers can be defined into multiple types of threats, their main type of threat is identified and described here. For example, the mere use of a computer does not automatically make an incident a cyberattack. If an individual intentionally shoots unarmed civilians for political reasons, they would be considered a terrorist. But if that same individual uses his company computer and authorized access to harm his company's physical property, they would be an insider. Lastly, that same person would be a cyber threat if they use their personal computer to gain unauthorized electronic access to unaffiliated information or systems.

Terror

Terrorism can pose the most serious harm to human life, personal injury and catastrophic property damage. These threats are typically carried out against civilians using everyday items such as knives and vehicles as weapons, as well as small arms and homemade explosives. More sophisticated terrorists are working to employ chemical, biological, radiological, nuclear and highly explosive (CBRNE) weapons of mass destruction. In order to be successful, these threats need to circumvent physical safety precautions and often carry political or religious motives. Sometimes, perpetrators possess a willingness to die for their cause. Recent examples of domestic terrorism in the U.S. include the attacks in Pittsburg, Parkland, Orlando and San Bernardino.

Note that terrorist attackers can fall under multiple treat types. The San Bernardino attackers, who carried out the Dec. 2015 shooting at the Inland Regional Center, could also be categorized as insiders, since they knew and worked with their targets. However, they are categorized as terrorists here, since they did not use company assets to conduct their attack and their primary motivation was political.

Cyber

Cyber threats, as defined here, come from external attackers without authorized access information technology assets. Perpetrators include foreign intelligence services (FIS), state-sponsored organizations, terror groups, organized crime and individual actors. Cyberattackers cover their tracks using the public Internet or telephone networks to circumvent perimeter network defenses. They then need to probe, map, navigate through and attack the internal networks, ICS/SCADA systems (industrial control system / supervisory control and data acquisition), computers and ultimately the internal information and assets. Tools include use of security vulnerabilities, overloading, cracked passwords, downloaded malware or stolen identities, for example. Damage is likely to be in the form of unauthorized access, violation of privacy, loss of intellectual property, theft of financial resources and other harm to intangible and tangible assets. Recent examples include cyberattacks on numerous U.S. government agencies, hospital ransomware attacks, Target, Sony, Cosmos Bank, JPMorgan, Equifax, Target and Yahoo.

Insiders

Insider threats, as defined here, come from individuals with authorized access to assets with the malicious intent to harm familiar people, physical property or computer systems. They are closest in proximity to their potential targets, with goals typically focused more on theft, extortion, revenge and embarrassment. However, insiders can also kill and injure co-workers and cause property damage. Recent examples of insider attacks include the Washington Navy Yard shooting, hospital ransomware attacks and infamous insiders such as NSA contractor Edward Snowden and Chelsea Manning.

Snowden and Manning are considered insider threats, not cyberattackers, since they had authorized access to the computer systems. Note, as used here, “authorized access” means electronic credentials rather than an approved need to know. Similarly, they would not be considered terrorists, since they targeted the U.S. government and not civilians.

The risks from insider threats have recently increased so much that the DOD’s Defense Security Service (DSS) published Change 2 to the National Industrial Security Program Operating Manual (NISPOM, aka DoDM 5220.22) on May 18, 2016. This change requires DOD contractors with classified contracts to establish an insider threat program that detects, deters and mitigates insider threats..

STEP 2: PRIORITIZE THREATS

The following models illustrate different approaches to prioritizing threats based on generic factors such as legalities, severity of harm, probability and proximity.

Legal, Regulatory and Contractual Liabilities

First and foremost is to comply with legal, regulatory and contractual requirements. The U.S. has a sectoral approach to legal requirements, where some sectors of the economy are governed by laws and regulations, while other areas are only voluntary. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires data privacy and security for medical information, but it does not apply to all confidential information. Similarly, the NISPOM Change 2 (discussed above) applies to cleared Department of Defense contractors but not to all U.S. government contractors.

Commercial companies and contractors working with the government in critical infrastructure areas, in particular, should pay close attention to those areas' very specific rules and regulations when making their calculations.

Liabilities to the U.S. government arise from failure to comply with laws and regulations applicable to your specific business. For example, the Federal Energy Regulatory Commission (FERC) requires some, but not all, transmission owners (depending on voltage and support to nuclear plants) to implement physical security plans customized based on the risk assessments of each individual station or substation in accordance with FERC's CIP-014. Similarly, the NISPOM applies to cleared defense contractors but not to all federal contractors, and the data privacy and security requirements for medical information under HIPPA does not extend to all confidential information. To mitigate liabilities to the government, companies need to fully understand all the requirements that apply to them, internally assess their current compliance and identify any gaps. Companies then need to prioritize and implement improvements as described below based on company-specific threats.

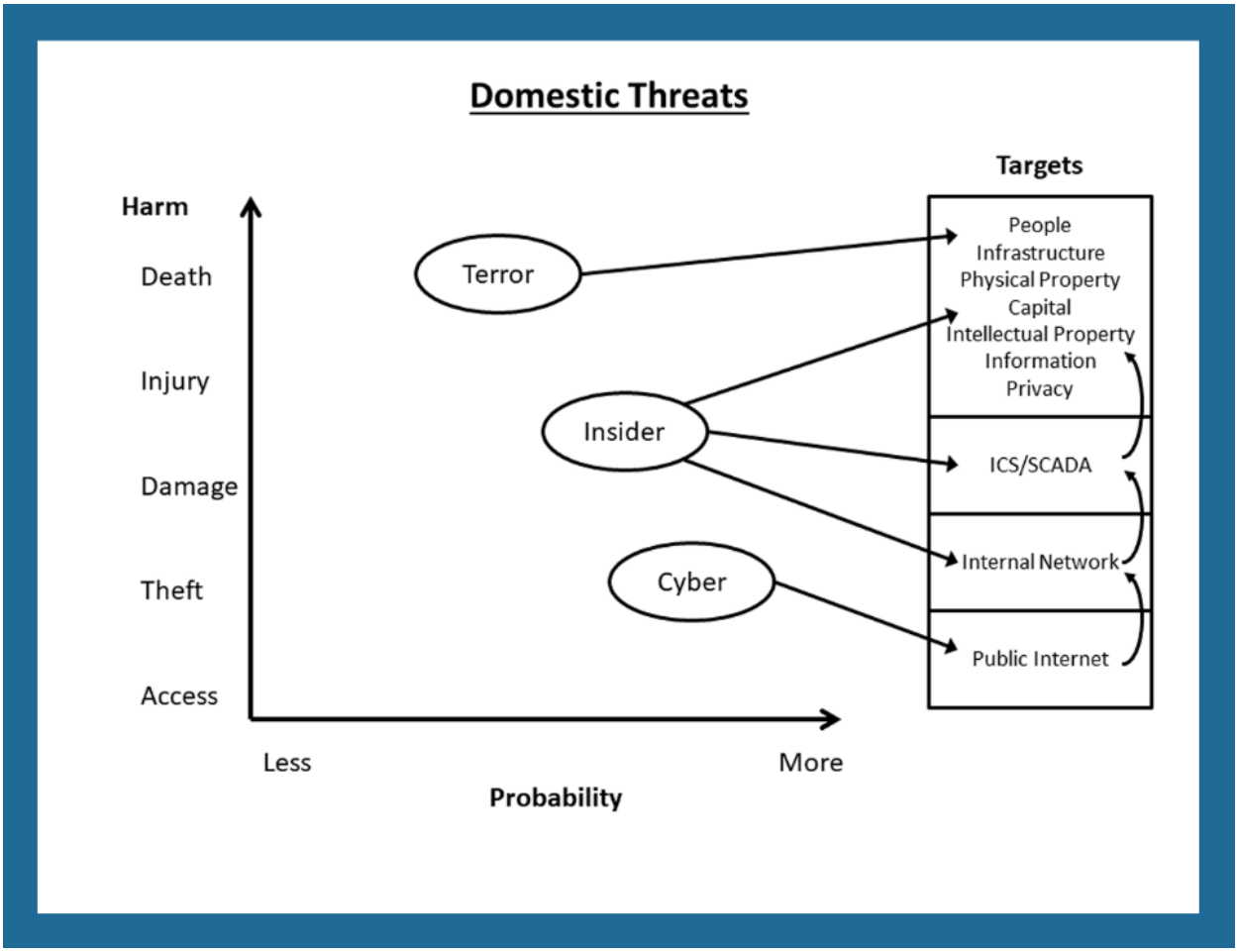
Liabilities to other businesses can arise from failure to comply with your contracts. Contracts can include express requirements to prevent unauthorized access to key assets. For example, the operator of sports centers may be contractually required to prevent unauthorized physical access, while a bank may be contractually required to prevent the theft of finances and a datacenter may be contractually required to prevent unauthorized access to the information. Failure to perform these tasks can lead to claims of contract breach, resulting in the payment of damages. These contractual liabilities can be mitigated with well-negotiated statements of work, inspections, service credits, liability caps, force majeure and other mitigation terms. Companies can further mitigate liabilities by quickly implementing the highest priority requirements first as described below.

Liabilities to private parties can arise when a company is negligent and does not take reasonably prudent measures which might have prevented successful attacks. But what are reasonably prudent measures? Real world events and industry norms change over time, resulting in these attacks becoming foreseeable. Terror and cyberattacks are, for example, in the news every day and increasing in numbers. This has the tendency to make these attacks more foreseeable, and at some point, depending on the jurisdiction, could result in new security measures being reasonably required.

The priority of threats based on these legal requirements would adhere to the express language of the law, regulation or contract, as well as the potential penalties or financial liability from their violation. Companies should fully implement countermeasures against the most serious threats while simultaneously beginning to implement countermeasures for the less serious threats.

Harm

Another way to prioritize threats is to look at the seriousness of harm such as death and personal injury, catastrophic damage to critical infrastructure, theft of tangible and intangible property and unauthorized access to personal information. Terror attacks deserve the highest priority of attention, since attackers aim to kill or injure people. Based on harm, insider threats rank second, since such attacks might target people but are more likely to target financial gain, physical infrastructure and confidential information. External cyber threats can cause financial harm, injury to brand, loss of intellectual property and invasions of privacy, but they are unlikely to kill or injure people or damage property.

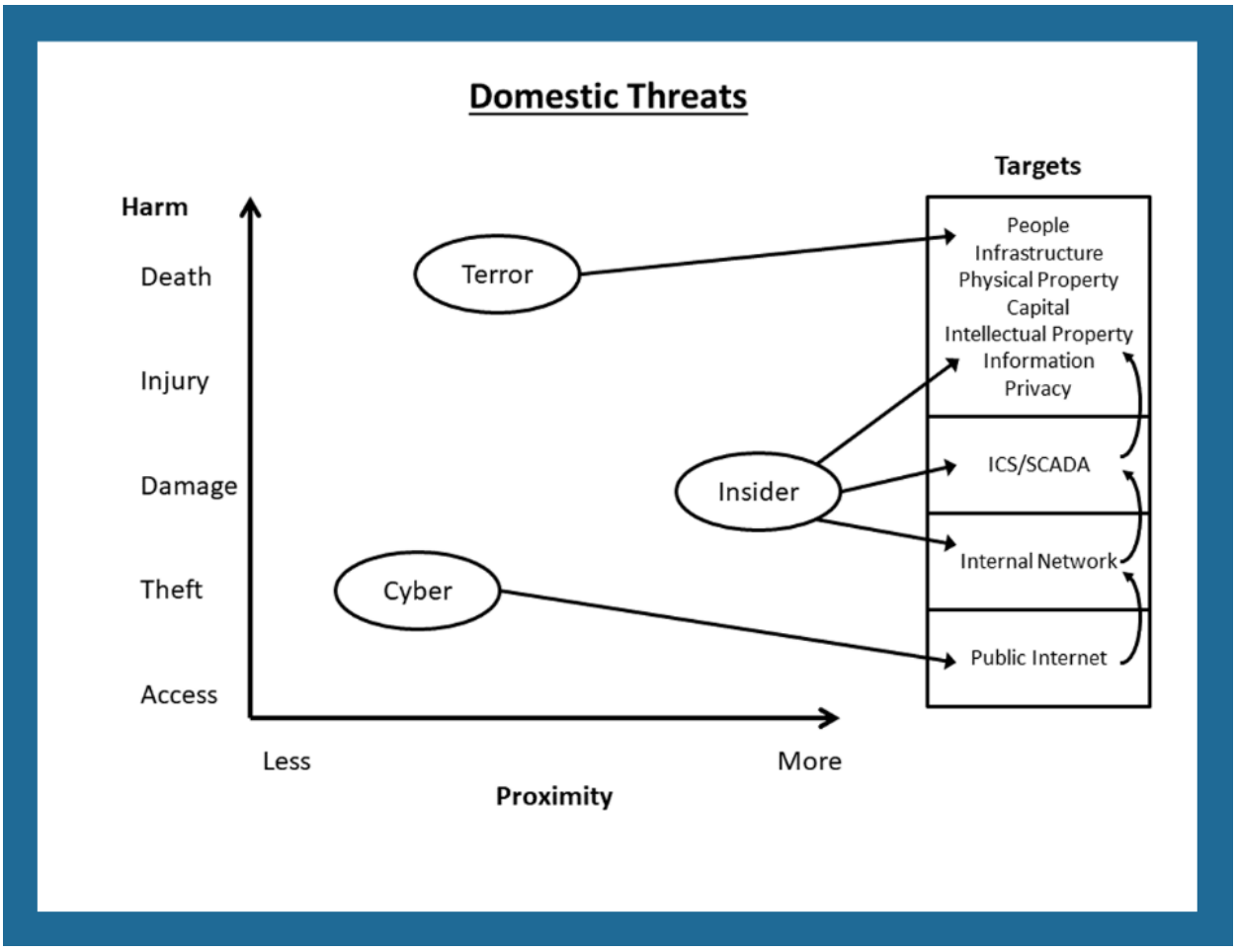


Probability

A third way to prioritize which threats should garner focus is based on the "probability" of an attack, defined here as the numeric quantity of each type of threat. The seemingly daily barrage of actual cyberattack reports shows that cyber is a high probability risk. Similarly, the prospect that every employee or contractor is a potential insider threat is a fact companies must keep in mind when prioritizing resources. Thus, based on the number of actual attacks, cyber threats are the highest priority, followed by insider threats. Terrorists, on the other hand, need to form extreme emotions and even to be willing to die for their cause and are fewer in numbers.

Proximity

A fourth way to prioritize threats is based on the "proximity" of the attacker, defined here as how close an attacker is to the target or how easily an attack can be made. Using this approach, insiders are the closest to their targets and can attack easiest since they already have authorized access and only need intent or carelessness. Terrorists are next, since they can simply walk or drive right up to an access point and employ commonly available brute force items to breach the perimeter and conduct an assault. Although cyberattacks only need a computer and internet connection, they are the farthest in proximity, since they are separated by long distances and the many intermediate steps, such as needing to defeat various levels of security and establish access to their targets.



STEP 3: CUSTOMIZE COUNTERMEASURES

In order to mitigate liabilities, the above generic prioritizations need to be adjusted in accordance with organization-specific variations and their primary assets. Different assets as targets should inform and revise how an organization plans for, prioritizes, protects and reacts to threats. For example: (i) the operators of public gatherings, community centers and sports stadiums would be primarily concerned with the safety of people; (ii) the owners of telecommunications networks or the electricity grid would be primarily concerned with the safety of the physical infrastructure; (iii) cleared government contractors would be primarily concerned with protecting classified and sensitive materials, equipment and facilities; (iv) banks would be primarily concerned with the security of their financial assets; and (v) a technology development company would be primarily concerned with the security of its intellectual property.

Protecting People

Protecting people from terrorism is likely to be a high priority to everybody, especially the operators of public facilities at which large numbers of people concentrate. Countermeasures against these terror threats would be more heavily designed for personal security, such as in-person questioning, real-time observations, ballistic perimeter fencing, vehicle barriers, secure doors, 24x365 armed guards, aerial drones, cameras, thermal imagery, night vision, motion detectors, x-ray and metal detectors, canines and more.

Protecting Financial, Privacy and Intangible Assets

On the other hand, protecting a brand, classified information, financial systems, intellectual property, privacy and other intangible assets from cyber threats would likely be the highest priority to government contractors, banks and technology companies. Countermeasures against cyber threats are focused on implementing best practices, hiring the subject matter experts who are effective security managers, purchasing and updating technical products and using modern services to secure information technology. Routine application of ordinary cybersecurity measures is paramount to reducing risks. These measures include keeping servers up-to-date, implementing appropriate boundary protections and using good endpoint protections.

Protecting Physical Property

Finally, protecting physical property from insiders would likely be the highest priority to the owners of critical infrastructure and equipment, such as the energy grid, telecommunication networks, IT systems and clean water sources. Countermeasures against insider threats would include some of the physical securities discussed above, but they could also be more focused on the human element to monitor, detect and investigate suspicious activities inside and outside places of business. This includes mitigating risks from allegiance to a foreign government, influence by a foreign organization, improper behavior, personal problems, financial troubles, sexual misconduct, alcohol and drug use, emotional disorders or misuse of IT systems.

NEXT STEPS

Prepare, respond and recover. Learn. Repeat.

This threat framework and comparative analysis is a solid start to allocating deterrence resources and mitigation efforts. However, it is only a start. Threats evolve and combine to attack numerous domestic targets. For example, terrorists might pull off cyberattacks that interfere with domestic politics and disrupt effective government, interrupting the delivery of critical infrastructure and basic services. These morphing threats demand innovative ways to assess and implement countermeasures.

Legal, operational and technical expertise should be engaged to analyze these risks, prioritize threats and implement mitigation measures. In addition to prioritization and tactical threat responses, organizations must negotiate proper service and equipment contacts, analyze organizational risks, address and develop corresponding regulatory compliance programs and mitigation strategies, create and implement internal policies, require internal training and enforce rights. Using and expanding upon these principles and framework should make it easier for you to integrate your legal, business and IT resources to develop consistent and effective countermeasures.

**Mark J. Maier, Shulman Rogers*

A retired U.S. Army Colonel, Mark Maier was NORTHCOM's emergency preparedness officer for Maryland and worked closely with law enforcement and public safety agencies. Together with his hands-on technology experience as an electrical engineer, Mark has keen abilities to identify, assess, mitigate and respond to risks.

Mark now chairs Shulman Rogers' Homeland Security industry group and the firm's Government Contracts and Technology Transactions practices. His military, engineering and business background enables him to quickly understand complex situations and achieve client goals in government contracts and commercial technology.

Contact Mark: 301.231.0945 | mmaier@shulmanrogers.com

