YOU'VE GOT A KILL CHAIN—NOW WHAT?

AN IANS CUSTOM REPORT

OCTOBER 2014

Sponsored by:

Contents

Overview

The Kill Chain model has taken the Information Security (Infosec) industry by storm, but the model isn't an end in and of itself. Rather, it's a means to an end, which specifically advises where and how to defend.

> ***Security is a strategic, system-wide property, and it requires a systematic approach.***

The value of the Kill Chain is that it illustrates how systems are being attacked today. In doing so, it gives defenders a range of choices on the most prudent ways to defend their systems. In an industry like Infosec that often focuses on the tactics, the Kill Chain is an important strategic decision-making analytical tool for linking threats to architecture risks and architecture risks to countermeasures. Security decision makers must educate the C Suite; graphical representations are useful here to communicate the current state of threats and vulnerabilities.

The Kill Chain addresses one of the prime weaknesses in field grade Infosec today. Consider the recent shellshock vulnerability. One vulnerability caused issues across the system as a whole. This vulnerability is very complex and far reaching. How do you explain it? How do you strategize around it? How do you identify the assets, business risk and use cases? You can utilize the Kill Chain approach, as we know there are not enough Security Architects to go around. Security is a strategic, system wide property, and it requires a systematic approach. This paper will look at the following topics:

- **Strategic Security** - Linking Risk to the Kill Chain model, and diving into how Chief Security Officers (CSOs/CISOs) and Security Architects use this analytical tool to improve security decision-making and investing
- **Using a Kill Chain** - How to use a Kill Chain improve your security posture

In addition, this paper will work to answer the following question; how do security decision makers get traction on longstanding problems in Information Security?

Strategic Security

> ***The goal of a Kill Chain is to improve security decision-making and investment.***

The goal of a Kill Chain is to improve security decision-making, proactively illustrate gaps and discuss the security investment. One of the most useful aspects of the Kill Chain approach is that it's a bottom up analytical tool. That means it has the context to map to the part of the system under attack and the measure used in the attack. But to be useful for CSOs and upper management, the Kill Chain is an input to a higher level of the CSO's decision-making process.

In "Investing in the Unknown and Unknowable"[1] Richard Zeckhauser distinguishes between operating in zones of Risk (probabilities known), Uncertainty (probabilities unknown), and Ignorance (States of the world unknown). He links those decision-making knowledge zones to the environment and skills needed to operate effectively.

There is a direct analogy between this type of decision-making environment and the one that we face in Infosec on a daily basis. As much as "Risk Management" is baked into almost every Infosec program, in fact in most cases we do not know the probabilities of attacks and impacts, and so we are not really managing risk. Instead we are managing through uncertainty and ignorance.

Infosec has both a Defender side and an Attacker side. In the case of the Defender, it's fair to make a case for many systems that we operate in a zone of Uncertainty. We do not precisely know the odds of events happening, but it is possible to define a range of events and outcomes. Even if we do not know the probabilities of one event or another happening, this is still a useful exercise to frame decisions.

On the Attacker side, it's fair to say in most cases Infosec operates in a zone of Ignorance, unknown unknowns. Will the new mobile application be attacked more or less than the older web application? Should we be more worried about internal or external attackers? How much do we trust the Cloud provider? Will mobile payments be more or less secure than traditional credit cards? These sound like existential questions, and they cannot be answered with 3 digits behind the decimal point level math. We do not precisely know the attacker's means, methods, and sometimes goals. Yet we still must make decisions on time and invest resources under these conditions.

Zeckhasuer's work is of high strategic value for security decision makers because while we sail under the "Risk Management" flag, we mostly do not know the probabilities of attack and strategic impacts. So we need to look to tools and processes that help us to operate effectively in areas where we lack probabilities and knowledge. Defenders live in the zone of Uncertainty for defenders and attackers dwell in the zone of Ignorance. The skills needed to get traction here include:

- **Portfolio Optimization** – CSOs and Security Architects manage a portfolio of security capabilities. Each purchase is in effect an investment that seeks to optimize your companies' security posture in response to an undesired outcome set.
- **Conjectured Distribution of Outcomes** – Unfortunately, there is not a simple, small list of things that can go wrong in computing environments. As

[1] http://www.hks.harvard.edu/fs/rzeckhau/InvestinginUnknownandUnknowable.pdf

every RISKS Digest list[2] reader knows, every day it's a security vulnerability parade.

When Infosec teams decide where and how to defend, how rational are these tradeoff discussions? The decision maker must decide what can be done via an automated tool versus ongoing consulting and professional services. The uplift from tools and automation plays a role in analyzing the total cost and efficiency of security capabilities.

A well-planned investment in a security budget line item should meet the following criteria. The security capability should mitigate a realistic threat. It should do so in the most cost effective and efficient manner. The Kill Chain provides insight in both of these. The Attacker lifecycle shows the distribution of threat activities. The Defender also gains an array of options for how best to defend. Combined, the outcome allows security decision makers to work toward a set of rational tradeoffs for how to invest in security capabilities.

Linking Risk to the Kill Chain

Kill Chains are a technology-centric view of how systems are attacked. Yet CSOs make their living based on how effectively they manage risk and technical risk is just one risk of many on their plates.

The Kill Chain model shows how attackers can get to Command and Control objectives against a target. This assessment should be fed into a risk assessment process that uses the Kill Chain to gain insight on ease of exploitability and downside impact if the threat's actions are successful.

There is a symbiotic relationship here. The Kill Chain informs the Business Risk Assessment processes and gives insight on relative probabilities and impact of technical risks. The Business Risk Assessment, in turn, helps to identify valuable assets, use cases, transactions, and deployments to focus the Kill Chain modeling work on those targets.

The CSO View

Most CSOs have a kind of "risk fatigue" brought on by dealing with more kinds of risk than they realized they were signing up for. What CSOs often lack is a systematic approach for dealing with risk, communicating risk management decisions and assigning responsibility and ownership in the organization. It's time to put the "C" in CSO and to do so, a structured approach is required.

It's time to put the "C" in CSO and to do so, a structured approach is required.

[2] http://catless.ncl.ac.uk/Risks

There is no “easy” button or silver bullet when it comes to managing Infosec risks. The CSO’s job is to support business initiatives that drive business revenue. That does not mean security gets a veto vote when something will drive double-digit revenue growth. If the business thinks that acquiring business revenue is the order of the day, then security can expect to be involved in the M&A review team, but it’s not likely the security posture of the acquired organization, however weak it may be, will be enough to scuttle the deal. In short, CSOs must deal with a wide variety of sub optimal scenarios.

The net result here is that flexibility and integration matter as much as anything in security today. The CSO cannot optimize the portfolio of IT assets to suit security’s goals because the IT portfolio is not owned by the CSO to begin with. Instead, CSOs must be able to adapt and find the most cost-effective place to defend the company’s assets and rally support from the business to do so.

The knock on effect is that a strategic approach must consider a range of possible options for improving security. Identifying the right mix of capabilities will vary from business unit to business unit and deployment to deployment. In that scenario, analytical tools that can show the range of possibilities and enable a rational tradeoff analysis are extremely valuable.

The Security Architect View – Taking Yes for an Answer

> ***The main problem now is not taking no for answer-- it’s taking “yes” for an answer.***

In 2014, the Security Architect’s job has really changed. In the past, Security Architects had to labor to get attention and inform the business that security is an issue. With breaches on the front page news every day, awareness that security matters is no longer a problem. The main problem now is not taking no for answer-- it’s taking “yes” for an answer.

Taking yes for an answer means that it’s not good enough to simply surface a problem. Executives are less concerned with details, but they are more willing than ever to invest time and resources in materially addressing security issues. The challenge for Security Architects today is how best to marshal those resources towards more security in real world deployments. Security conferences are replete with showing how things break, but now is the time to double on defense. The question that matters now are *where* and *how* to deploy controls and capabilities?

Using a Kill Chain

When things go awry, managers don't care too much about why they happened— they want it fixed. Take a stroll at any security tradeshow and there is no shortage of security “solutions” but it is not obvious which ones are the right

fit for your company's specific architecture and systems. Furthermore, which ones have the automation and scale that you'll need to run your team?

Kill Chain models help to answer these questions during an incident post mortem as it is a method for identifying security architecture design flaws and discussing security posture solutions and tradeoffs.

The Kill Chain concept is described in work by Hutchins, Amin, and Cloppert[3]. The authors lay out a seven step model for how systems are attacked:

1. **Reconnaissance** – Target selection
2. **Weaponization** – Customize payload
3. **Delivery** – Email, USB, Web
4. **Exploitation** – Execute payload
5. **Installation** – Remote backdoor
6. **Command and Control**
7. **Actions on Objectives**

The point of the Kill Chain concept is to identify where and how to best defend your system. The authors give a good example of layering different styles of defense to detect, deny, disrupt, degrade, deceive, and destroy potential attacks.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

[3] http://papers.rohanamin.com/wp-content/uploads/papers.rohanamin.com/2011/08/iciw2011.pdf

The two main valuable concepts that the Kill Chain approach provides are that it establishes a behavioral model for attackers that can then be used to specify defensive posture and security capabilities. The mapping in the matrix above shows that the combination of the attacker's phase through the lens of the defender's goals yields a fundamentally different set of controls and capabilities.

There is a long list of security capabilities that offer the possibility to improve defensive posture, but understanding where and how these best fit is a must. Network Based and Host Based intrusion detection (NIDS and HIDS), Data Execution Prevention (DEP), access control improvements like chroot jails, and Audit logging all have a role to play in an overall architecture. It's important to be able to put these in the context of an overall plan.

The attacker's lifecycle is discussed in different variants in many Hacking books and articles. The Kill Chain model presents one approach to demonstrate how determined attackers look to proceed.

The Kill Chain model also provides a model for how defenders act. This is far less studied. Defenders can look to accomplish a variety of goals to thwart attacker actions:

- Detect Activity
- Deny Access
- Disrupt delivery and execution
- Degrade attacker's usage
- Deceive attackers on progress toward their goals
- Destroy attacker capabilities

The combination of the attacker's lifecycle with the defender's menu of capabilities brings real world information security into focus.

How to Use a Kill Chain to Improve Your Security Posture

The Kill Chain gives Security Architects a broad and deep perspective on defending their systems. The bottom up model does not make any major assumptions that the best answer must be XYZ; rather it's a way to "see" what opportunities present themselves. Most security professionals talk about "defense in depth", but the Kill Chain gives you a way to design and make smart cost effective choices to build it inclusive of a way to view lateral movement and defend against it. This paradigm of lateral movement is not addressed in typical "defense in depth" strategies.

It's important to note that Kill Chain models should not be looked at as a "checkbox Olympics" where analysts slavishly ensure that they have an answer in every single box. Instead, it is a multiple step process which starts by using the

model to define the security opportunity set. The next step is to review the Kill Chain model to identify the most cost effective and high impact security controls.

> ***… to "defend" is not one single course of action; it's a set of capabilities planned from an array of possible choices.***

Finding Opportunities

The process of finding opportunities to deploy the countermeasures that the Kill Chain uncovers is a subjective, risk-based assessment. The inputs to this process include:

- Data sensitivity
- Transactional value
- Data flow analysis
- Data Storage
- Software architecture analysis
- System architecture analysis

These analysis steps show the valuable assets in systems that are the targets of the attackers. In addition, the foundational elements and any other dependencies that the assets rely on should be analyzed and factored in to the model. This can include host, application, network level assets, as well as related components like access control mechanisms, keys, and storage.

To define what capabilities in the Kill Chain are the best candidates to invest in, the next question is efficacy. How effective is the control at mitigating the threat action? The known set of attacks should be compared against the possible countermeasures that can meet the Defender goals such as Detection, Denial, and Disruption.

It's important to note that there is a difference in scale in most cases for where controls are deployed. Centralizing detection in gateways can give the broadest visibility, but certain access control decisions may require distributed deployments. The role of the security architect is to design the most effective mix.

Opportunities can be classified at a high level in two ways:

- **Raise the Floor** – Improve the minimally acceptable posture for certain elements in the security architecture
- **Raise the Ceiling** – Fundamentally improve the structure and/or behavior of the security capabilities

Well thought out security architectures should have the means to accomplish both of these goals, but the way to achieve them varies. Raise the floor could include Data Execution Prevention and Ad6jgdress Space Layout Randomization controls which improve the systems' resilience to certain kinds of attacks. On the other side, wiring up a Mobile application to use the biometric, fingerprint reader on iPhone and Android devices could fundamentally improve mobile authentication and raise the ceiling on what is possible for business applications in your enterprise.

Conclusion

A key point here in 2014 is that to "defend" is not one single course of action; it's a set of capabilities planned from an array of possible choices. The role of the security decision maker is to consider the range of options available based on the broad a set of threats systems face today.

The CSO should expect to proceed more like a mutual fund manager, building a portfolio of controls that can stand the test of time. The Security Architects charged with system design should be flexible to consider what Detection, Denial, Disruption and other capabilities deliver the best mix of automation, management, coverage and control for the platform.

The domain of Information Security is decades old, but the practice of rational security investment and design planning is in its infancy. Analytical tools like the Kill Chain model— especially when combined with Threat Models, Data Classification, and Business Risk Assessment— provide a crucial decision support to mature this discipline.

About Websense

Websense, Inc. is a global leader in protecting organizations from advanced cyberattacks and data theft. Websense® TRITON® comprehensive security solutions unify web security, email security, mobile security and data loss prevention (DLP) at the lowest total cost of ownership. Tens of thousands of enterprises rely on Websense TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware. Websense prevents data breaches, intellectual property theft and enforces security compliance and best practices. A global network of channel partners distributes scalable, unified appliance- and cloud-based Websense TRITON solutions.

About IANS

IANS is the leading provider of in-depth security insights and decision support delivered through research, community, and consulting. Fueled by interactions among IANS Faculty and information security practitioners, IANS' experience-driven advice helps IT security, risk management, and compliance executives make better, faster technical and managerial decisions.

IANS was founded in 2001 as the Institute for Applied Network Security. Inspired by the Harvard Business School experience of interactive discussions driving collective insights, IANS adapted that format to fit the needs of the information security community.