THE 405(d) POST

Volume 1

A Word From the Task Group

A Simple Model to Discuss Cyber Risks with Executives

Erik Decker, Task Group Lead

Welcome to the first issue of the 405(d) Post. I hope this article won't be yet another 'big think, high concept, and no meat' piece. How many conferences, dinner events, or seminars have you attended, and how many articles have you read that have an enticing headline but leave you wanting?

First, a little bit about me. I have the privilege of serving as the Chief Information Security Officer and the Chief Privacy Officer for a large academic healthcare institution. I also have the honor of serving as the industry lead of the Cybersecurity Act of 2015 405(d) Task Group, with my government counterpart, Julie Chua, of the U.S. Department of Health and Human Services.

So now that I have your attention, I think you're ready for the model, right? Let's get right down to it.

Model

I'm going to keep this very simple and easy to follow. I will start with my first caveat; nothing is this simple when it comes to executing your cybersecurity strategy. However, this model isn't designed for how you are going to execute your security program. Rather this is a way you can communicate to your executives about how to discuss cyber threats and risks, and what to do about them.

Another quick note – in this article I am going to focus solely on a simple threat model, a simple risk model, and a set of techniques about "what to do about it." We are not going to discuss Risk Analysis processes or Roadmap exercises, however, those are the next logical conclusions after you've done your prep work.

Threats

There are a lot of ways to think about threats, and for those in the trenches, threats can be too numerous to count. However, for the purposes of explaining complicated cyber issues to your executives, I like to break threats down into two components: Intent and Proximity. Your threat actor's motivations may be malicious or they might be accidental; they could also be internal to your environment, or external.

In This Issue

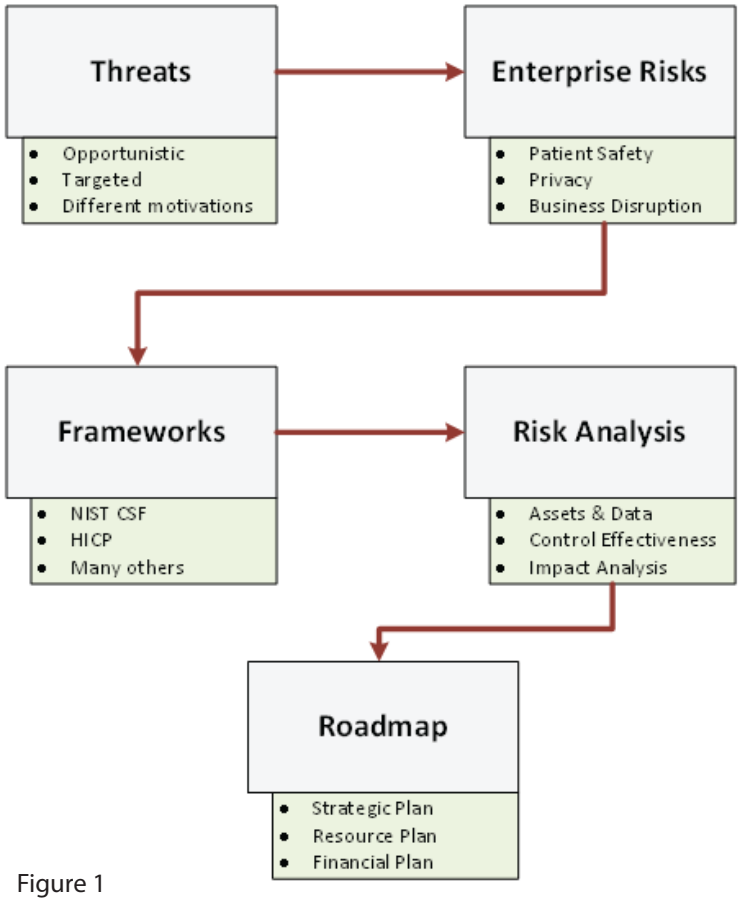


Figure 1

Figure 2

Threat models get more complicated than this, but it's a place to start. The next part of the conversation could be the context of these threats: who are these threat actors and what types of actions do they take? The hacking that occurs today has changed dramatically from the hacking of old. Twenty years ago the malicious hacking community tended to be small groups of individuals who had limited resources to cause havoc. Today we have an entire underground service industry, "Hacking for Hire," that has emerged and placed everyone at risk. With the dramatic increase in the level of sophistication and the lower bar of 'entry' to start a hack, the risks have proportionally increased.

This is the reality, but how do you convey that complexity to the executive team? I posit a simple matrix. On one axis you can group your threat actors into five simple categories which range from 'limited resources' all the way up to 'unlimited resources' (nation states). Clearly the level of defense to combat a lone hacker is quite different from that needed to combat a nation state.

On the other axis are the actions that these threat actors take. Generally speaking, you have either malicious actions (such as targeted attacks or opportunistic attacks) or unintentional actions (such as an employee mishandling data that exposes sensitive data). The intersections between these actions can provide an orientation on the threat actor's motivation. So let's look at a few examples below.

	Threat Actions			
	Economic / Disruption			Pt. Safety
Threat Actors	**Targeted (Specific Victims)**	**Untargeted (Indiscriminate)**	**Accidental**	**Medical Devices**
Individuals / Small Groups	Data Theft	Data Theft	Data Mishandling	
Hacking Groups	Reputational Embarassment	Data Theft Political		
Organized Crime	Extortion	Extortion Data Theft		Physical Harm
Terrorism				Physical Harm
Nation States	Political Espionage	Disruption		Physicial Harm

John Doe is an employee of ACME Medical, working in the revenue cycle office. John is working on compiling a list of all patient cases over the last quarter, which includes their names, diagnosis information, insurance data, and costs of care. He's doing this at the request of management. John finishes his compilation and sends the data in an internal email. Unfortunately, he mistypes the email address and selects a listserv from a professional association he works with because it popped up as a 'suggested recipient.' One thousand records get sent to the members of this listserv. Oops!

Threat Actor: Individual; **Threat Action:** Accidental; **Motivation:** Data Mishandling

ACME Medical is known to care for some very prominent persons of public interest. Being located in the greater Washington, D.C. area, there are certainly a number of high-profile political figures that receive their care at ACME. This is of particular interest to the country of Malintentopia, who is quite upset with the United States. In an attempt to get political leverage and potentially blackmail certain prominent figures, Malintentopia hacks into ACME Medical and uncovers a very sensitive diagnosis of a senior member of the White House which would put their job at significant risk. They use this intelligence for blackmail.

Threat Actor: Nation State; **Threat Action:** Targeted; **Motivation:** Political

To see some of the common tactics these threat actors use to conduct their threat actions, take a look at the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.* The document outlines five common threat tactics that plague the health industry.

As you can see, these two scenarios are quite different from one another, but ultimately relate back to the same systems and organization. Additionally, the methods you would choose to protect against these types of attacks are quite different. So how do you do it?

Risks

You are the head of security for your health system and you're responsible for a whole bunch of patients, as well as your organization. You've been to all the conferences, you've gotten all the threat briefings, you read the paper, and you hear the horror stories. Everywhere you look you see a vulnerability; you see how it can all come crumbling down. You are part of the Matrix.

That's the problem – there is too much information and all problems are not equal. If you try and take this on a case-by-case basis you will exhaust not only yourself, but also your team. If you try and communicate the issues to your executives on a case-by-case basis, you'll find that initially there will be a lot of anxiety and action, then exhaustion, and then finally folks will stop listening. This is a Chicken Little-free zone.

At this point the skeptics are thinking "it's not simple, Erik." I know; I'm with you. I offer you this, however, as a suggestion. At the end of the day, with all of the problems that can arise, what are the impacts that we care about the most? There's not many, when you get down to it. Sure, there are variations on the impacts that can be made, but what an executive cares about is "what could go wrong," "what's really the chance this could happen," and "what are we doing about it."

First off, and this is not new thinking, ultimately risk can be broken down into a simple formula. There are several of them out there; I'm not going to tell you which is best, but instead I'll just highlight a few:

- Threat x Impact = Risk
- Threat x Likelihood x Impact = Risk
- Threat x Vulnerability x Consequence = Risk

Notice a theme? Threats are always there. As such, I give you, at the core, three risks that *most* health systems in the world faces:

Risk	Description
Business Disruption	The potential for attacks against your digital assets that shut down the ability for your organization to operate and provide care. In some cases this might be specifically shutting down services; in other cases the attacks might attempt to 'ransom' you to get your organization back up and running. This isn't about the data; this is about care delivery and your operations.
Patient Safety	The potential for harm to occur against your patients through the digital ecosystem. This could occur maliciously by an attack on a connected medical device; however, it could also happen by shutting down the ability to care for your patient or by having 'bad data' inside key clinical systems.
Privacy	The potential for a loss of confidentiality and privacy of your patient information which could cause financial implications to patients or reputational implications and embarrassment to your organization. This is the traditional concern the health industry has been focused on for decades.

** Note: these definitions were created by Erik Decker, not sourced from any particular source

There are more risks than these, certainly. There are other things that might be relevant to your executives that are outside the core of these three risks. For example, you might be going through a fairly aggressive growth strategy and you're buying up other hospitals. That expansion and footprint increases the risk landscape, and the methods you would use to manage that might be different from general cyber risk management. Feel free to add methods and adjust them as you see fit!

Notice that I didn't quantify these risks or provide any level of priority to them. That's up to you; you certainly can't just list a risk and start your planning. Additionally, the level of susceptibility for these risks will vary between organizations. You could be a nationally recognized health system and be under constant attack by a nation state, or you could be a small safety net hospital that isn't on anyone's radar. The important thing to note, however, is that we all have some exposure to these three risks.

Frameworks and Management Techniques

Okay, you got through my models – you might agree with them or you might think they're too simple. Feel free to pick and choose what works for you and throw the rest out. At the end of the day, the point of this risk management activity is to group your areas of weakness, prioritize them, and *then do something about it.* That is where your frameworks, controls, practices, and management techniques come in.

First and foremost, when building out a security program, it's really important to understand what the 'whole program looks like.' That's where frameworks come in to play. I recommend you take a good, hard look at the NIST Cybersecurity Framework (CSF). It's quite comprehensive in its nature, it provides a good level of detail that describes the 'outcomes' of what the elements of your program should look like once implemented, and gives you a start and end. If you can't frame up what your program does, how else are you going to organize, plan, and deliver your work?

The NIST CSF also gives you, with its Tiering mechanisms, a nice and easy way to explain to your executives where you are on your journey towards managing these risks. My suggestion is to directly map back the high-level risks I posited above to the framework of your choice, and then measure yourself against that framework. It is an elegant way to demonstrate your mitigation capability on a maturity scale and an easy way to show the executives where you are in your journey.

That all sounds quite fancy and high-level, doesn't it? Sounds like you could put that into a PowerPoint presentation, polish it up, impress your executives with your understanding of the world of cyber, and walk away feeling good. However… what do you do then? If you stop there you're a sitting duck!

This is the place where the *Health Industry Cybersecurity Practices: Managing Threat and Protecting Patients* can help. This guide was specifically written to give you actionable, practical, and measurable advice on how to implement key cybersecurity practices that will directly mitigate the threats and risks I discussed above. One hundred fifty of your peers debated, twisted arms, and scrutinized the best ways to offer specific suggestions to small, medium, and large organizations. Consider it your 'cyber cookbook' that provides you with recipes and instructions on how to "make" your core cybersecurity. Give it a read and have that 'ah-ha' moment (e.g., "so THAT'S what a Security Operations Center does" and "THAT'S how I can build a playbook. Cool!").

Conclusion

As I mentioned at the start, I left out the Risk Analysis process and the Roadmap process. Suffice it to say, once you've classified your threats, determined how they influence your risks, and selected your framework for managing it, you're well on your journey towards building your plan. By keeping these discussions simple and modeling only a handful of threats and risks, you'll see that understanding come together with your executives.

Good luck!

HICP Spotlight

Two-Factor Authentication to Safeguard against Email Phishing Attacks

Email is the primary mechanism used by most health care organizations to communicate electronically and it's common to share sensitive information through email systems. It's also common to access email remotely, especially as the workforce has become increasingly mobile. From practitioners sharing patient information or hospital administrators processing records from a remote location, email systems can be vulnerable and are the number one target for hackers.

In credential harvesting attacks, hackers use phishing tactics to obtain email passwords and login credentials from remote email systems. Given the prevalence of credential harvesting attacks, passwords are the only controls prohibiting malicious users from accessing sensitive information within transmitted emails. This is a critical exposure that increases an organization's susceptibility to phishing attacks.

Tip of the Month

Be sure to double check email addresses when being asked for login credentials or for payment processes. If you suspect an email may not be from the intended sender there is always the option to give them a call and double check!

Two-factor authentication, or multifactor authentication (MFA), is the process of verifying a user's identity using more than one credential. ***This is one of the most effective controls to protect your organization's data.*** The most common method is to leverage a soft token in addition to a password. A soft token is a second credential that can be delivered through a second device (i.e., mobile phone or tablet). The soft token could be, for example, a text message containing a code or an application installed on the user's mobile phone that provides the code and/or asks for independent verification after a successful password entry. Implementing MFA on a remote-access email platform mitigates the risk of a compromised credential and would decrease the likelihood of being hacked due to compromised credentials while working from a remote location. With MFA, a hacker needs to obtain the user's password and soft token, which significantly reduces the likelihood of a successful attack.

To learn more about MFA and other practices used to prevent email phishing attacks, visit the 405(d) website and the full HICP Publication.

405(d) Announcements

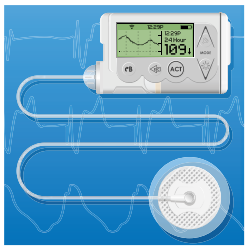
FOM/IT Conference October 24-25 in Chicago, IL

Join 405(d) Federal Lead Julie Chua and Industry Lead Erik Decker at the FOM/IT Conference in Chicago for a panel discussing the importance of cybersecurity as an Enterprise Risk Management issue and how HICP can be used by all organizations.

Spotlight Webinar Series kicks off Wednesday October 9th!

Happening Around Us

U.S. Food and Drug Administration Warns Patients about Medical Device Vulnerability



On June 27, 2019, the U.S. Food and Drug Administration (FDA) released a statement warning patients and health care providers that certain Medtronic MiniMed insulin pumps are being recalled due to potential cybersecurity risks. The recall comes as growing concerns over potential cyber threats against these devices is on the rise. The FDA is concerned that a hacker could wirelessly connect to the device and deliver the wrong amount of insulin. The HICP Publication specifies attacks on medical devices as one of the five major threats currently facing the health care industry.[1]

Check out the HICP Publication to learn about practices used to prevent these types of attacks.

Oregon Department of Human Services becomes Victim of Extensive Phishing Attack

The Oregon Department of Human Services (ODHS) fell victim to a phishing attack this January, resulting in 645,000 compromised victims. Unfortunately, it took ODHS and Oregon's Department of Administrative Services' Enterprise Security Office nearly three weeks to detect the hack. Once ODHS officials determined that protected health information was involved in the cyberattack, officials updated the website's breach notice on March 21, 2019.[2]

This incident reinforces the importance of training and proactive practices to prevent against email phishing attacks. Check out the HICP Spotlight to learn about a common practice used to stop these attacks before they happen.

Small Health Care Provider in Ohio Pays $75,000 in Ransomware Attack

Ransomware is increasingly prevalent, and high ransoms greatly affect smaller practices. NEO Urology was hit by a severe ransomware attack that infected its entire information technology system. Due to the complexity of the hack, the Ohio health care provider paid the $75,000 ransom. The hack was so severe that after the ransom was paid it took three days for the practice to regain access to its computer systems. In addition to the paid ransom, NEO Urology reported between $30,000 and $50,000 per day of revenue loss.

During the first quarter of 2019, ransomware attacks on business targets increased by a staggering 195%, with 71% of these attacks targeting small businesses like NEO Urology.

The HICP Publication identifies ransomware as one of the five major threats facing the health care industry today. Read the full HICP Publication to learn about practices used to avoid these attacks.

HHS Topics and Resources

HEALTH SECTOR CYBERSECURITY COORDINATION CENTER
A Health Sector Prescription for Cybersecurity

Health Sector Cybersecurity Coordination Center (HC3)

Business Email Compromise (BEC): Deception and Theft

https://content.govdelivery.com/attachments/USDHSCIKR/2019/03/15/file_attachments/1174076/HC3_Business%20Email%20Compromise_20190313.pdf

The Office of the National Coordinator for Health Information Technology

Office of the National Coordinator for Health Information Technology (ONC)

Trusted Exchange Framework and Common Agreement
https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

Assistant Secretary for Preparedness and Response (ASPR)

Technical Resources Assistance Center and Information Exchange (TRACIE)
https://asprtracie.hhs.gov/

FDA U.S. FOOD & DRUG ADMINISTRATION

Food and Drug Administration (FDA)

Pre-Market Cybersecurity Guidance (Currently in Drafts)
https://www.fda.gov/news-events/fda-brief/fda-brief-fda-proposes-updated-cybersecurity-recommendations-help-ensure-device-manufacturers-are

HHS 405(d) Aligning Health Care Industry Security Approaches

Contact Us!

www.phe.gov/405d

CISA405d@hhs.gov

[1] https://www.fda.gov/news-events/press-announcements/fda-warns-patients-and-health-care-providers-about-potential-cybersecurity-concerns-certain

[2] https://healthitsecurity.com/news/breach-tally-of-oregon-dhs-phishing-attack-reaches-645k-patients

[3] https://healthitsecurity.com/news/ohio-provider-pays-75k-ransom-after-serious-hack-on-it-system