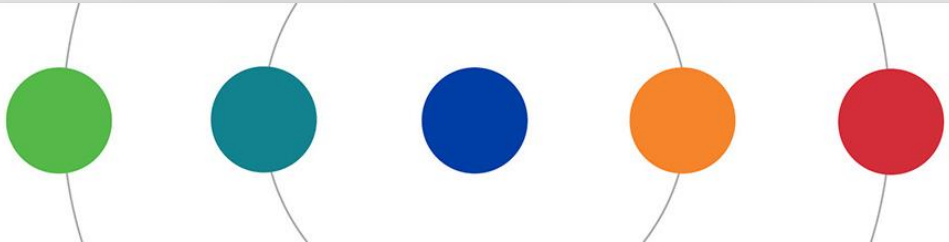
MAYO CLINIC

Information Security Operations and the Advanced Persistent Threat

Singapore Healthcare Management 2020

Andrew Coyne, CISO, Mayo Clinic

18th August 2020



1. Introduction

1.1 Mayo Clinic

- Mayo was founded in 1889 and is now a leading nonprofit international academic medical center.
- Primary principle: “The needs of the patient come first”.
- Over 4,800 physicians and scientists; over 60,000 other staff; 1.3 million visits from 138 countries; 129,000 admissions.
- Major campuses in Minnesota, Florida, and Arizona, and a regional health system of 19 hospitals.

1.2 Quick Introduction

- Chief Information Security Officer (CISO) serving Mayo Clinic.
- Previously with a big four consulting company, developing information security and privacy programs for Fortune 500.
- Born in the UK. Worked in SG. Living in the US.

1.3 Session Summary

- The Advanced Persistent Threat (or APT) means the sophisticated state-sponsored hacking units practicing espionage around the world.
- China, Russia, North Korea, and Iran have all been implicated in these attacks. Healthcare has seen major APT attacks in recent years.
- Now, during the Covid-19 emergency, APT hackers are targeting institutions involved in the global response to the pandemic.
- We will discuss the nature of the threat, and consider some common-sense steps we can all use to help protect our institutions.

2. Great Power Rivalry & International Espionage

2.1 Setting the stage

- **The long peace**: The great powers have avoided *major* wars since 1945. Deaths caused by war have declined yearly.
- **Reasons for peace?** Some have suggested nuclear deterrent, lucrative global trade, greater democracy, the empowerment of women, peacekeeping by the UN, and reduction in poverty.
- **War went underground:** It's not all rainbows and unicorns. World powers have continued to compete through espionage.

2.2 Motivations for espionage

- **Projecting power:** Countries see espionage as an effective tool for projecting global power.
- **In a hurry:** Some countries are concerned about the current world order, and seek urgently to become world powers.
- **Cold War lessons:** Developed countries have more advanced technology. Espionage is seen as an effective means to skip decades of expensive R&D and “close the gap”.

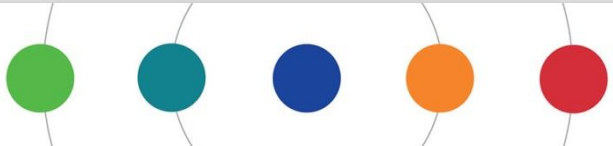
2.3 Espionage probably won't go away soon

"The Great Game is finished when everyone is dead. Not before."

– Rudyard Kipling, *Kim*

2.4 Espionage in the age of the internet: The APT

- **The great equalizer:** The internet has made espionage (and sabotage) easier, allowing any nation to cheaply reach institutions and infrastructure across the world.
- **Intelligence:** During times of peace, espionage of all types provides a way to obtain intelligence about adversaries.
- **Sabotage:** During times of war, espionage of all types provides a means to sabotage adversary critical infrastructure.

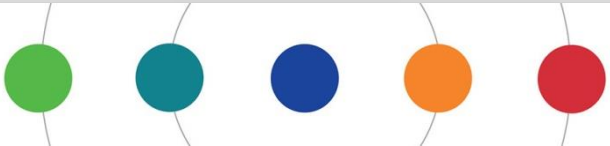


3. The APT, or "Advanced Persistent Threat"

3.1 China denied internet spying in 2013

“It is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence.”

– Chinese Defense Ministry, January, 2013.



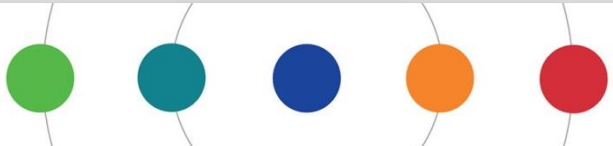
3.2 The US eventually offered grudging respect

"You have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute."

– James R. Clapper Jr., US Director of National Intelligence, June, 2015[1].

3.3 The first APT group revealed

- **APT1:** The American cybersecurity firm Mandiant released a report in February 2013 implicating China in cyber espionage[1].
- **The report:** Mandiant exposed the tactics, techniques, and procedures of PLA Unit 61398, codename “APT1”.
- **Exposed:** The report included photos of PLA hackers, videos of their hacking activity, even the building they operated from.
- **Acquired:** In 2014 Mandiant was bought by FireEye for $1B.



3.4 Identification of more APT teams followed

- **More hackers:** MITRE currently tracks 109 sophisticated APT-type groups involved in global cyber threat activity[1].
- **International:** FireEye highlights specialized state-sponsored from Iran, China, North Korea, Russia, and Vietnam.
- **Spy vs Spy:** Russia-based Kaspersky adds the so-called "Equation Group", alleging a US NSA connection.

3.5 Do we really know what we think we know?

- **Attribution:** Cybersecurity investigators attempt to attribute attacks to APT groups by analyzing attacker tools, tactics, and techniques. This is reasonable, but not fool-proof.
- **e.g. Moonlighting:** Some state-sponsored APT hackers are suspected of moonlighting, making attribution difficult.
- **e.g. False flag:** False-flag operations are designed to create a false attribution, to cast blame elsewhere and avoid reprisals.

3.6 What do the APT groups want?

- **Objectives:** APT hacking groups from Iran, China, North Korea, Russia, and Vietnam have a range of goals[1]:
  - Theft of intellectual property and research from targeted industries, governments, and militaries.
  - Theft of business competitiveness information such as contract terms, M&A plans, etc.
  - Targeted surveillance of individuals.

3.7 Did hostilities escalate in 2015?

- **June 4th 2015:** Serious breach detected at the United States Office of Personnel Management (OPM), including highly-sensitive data from background investigations, impacting millions of Americans[1].
- **June 12th:** Chinese stock market crashes, losing **US$3.2TN** in just a few weeks[2].
- **July 8th:** NYSE halted trades for 4 hours after "technical glitch"[3].
- **July 8th:** United Airlines flights were grounded for hours after "a computer glitch"[4].
- **July 29th:** Bloomberg reports that those same Chinese hackers responsible for the OPM breach had already breached United Airlines back in June[5].

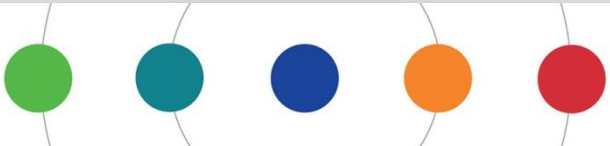
Caution: It *might* be wild speculation to connect all these events.

3.8 This senator joined the same dots

1

3.9 The cyber truce of 2015

- **Gentlemen's agreement:** In September 2015, Obama & Xi agreed not to sponsor hacking activities[1].
- **Pivot from China:** Chinese APT groups are believed to have pivoted from direct attacks on the US, instead focusing on Russia and Asian nations.



3.10 Resumption of China-US hostilities?

- **Caught in the act again:** By December 2019 Bloomberg was reporting[1] that Chinese APT20 were operational again, after appearing to have been dormant for years.

4. APT are Groups Exploiting Covid-19

4.1 Exploiting Covid-19 through users

- **Phishing attacks:** With the change to remote work, attackers are using fake emails to get “clicks” and access. Examples include fake PTO requests, fake medical leave forms, fake resumes.
- **Exploitation of Contract Tracing Apps:** Fake apps are used to gain access to your phone. For security, only use trusted software from known sources.

4.2 Exploiting Covid-19 through systems

- **VPN and Remote Access:** Many IT teams have had to rapidly scale remote access and VPN (virtual private network) systems during the crisis, possibly leaving vulnerabilities. Upgrade and patch critical systems.
- **Web vulnerabilities:** An uptick in scanning and attacks has been reported on websites, portals, and management interfaces. Again, upgrade and patch everything.

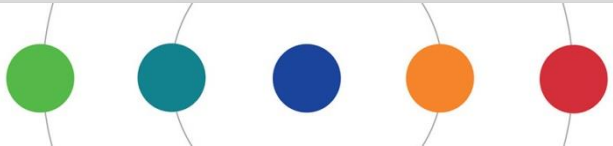
5. Security Operations: How To Respond

5.1 Are you a target?

- **Patient Data:** If your institution sees patients that work in government or defense you're probably on someone's list.
- **Research:** If your institution is involved in new and important research, you're also a likely target.

5.2 Do you care if you're a target?

- **Scarce resources:** Healthcare leaders are responsible for allocation of scarce resources. Should you even be focused on advanced threats?
- **Basics first:** If relatively common malware and ransomware still hurt your institution, you need to focus on getting a basic security program in place. See the Appendices for more information on pitfalls and approaches.

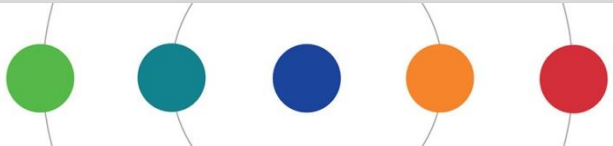


5.3 Prioritize your threats

- **Know your list of threats:** As executives, leaders, and members of governance groups, we should know the cyber threats that face our institutions.
- **Prioritized threat list:** Ask your cybersecurity people or consultants to produce a one-page ranked list of 5-6 cyber threats, describing the types of attacks your institution should care about, explaining why these threats, and not others.

5.4 Assume a state of breach

- **Be realistic:** If your institution is a likely target, you either have a superb, modern cybersecurity program benchmarked against leaders, or you may already have lost data in various ways.
- **Separation:** Think about additional protection you could apply to your most important data. Consider keeping your most important information in a separate system or “network segment” with additional monitoring.

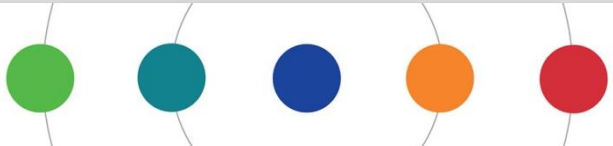


5.5 Fire engines vs building codes

- **Preparedness:** Make sure you have an excellent incident response program, and practice, practice, practice.
- **Become excellent at putting out small fires:** Your security operations people need to be excellent at dealing with “commodity” security incidents, ahead of the big one.
- **Systematically improve your IT quality:** See the appendices for approaches to improve IT hygiene.

5.6 Getting into the technical weeds (just a bit)

- **Incident response process:** Review and refresh your incident management processes.
- **VPN and remote access:** Apply the latest updates and patches to your VPNs, network infrastructure devices, and devices being used to connect into work environments.
- **Management interfaces:** Protect the “management interfaces” of your critical operational systems.



5.7 Getting into the technical weeds (just a bit more)

- **Multifactor:** It shouldn't need to be said at this point, but a username and password should be insufficient to get into your systems from "outside". Insist on multifactor authentication.
- **Replace the old stuff:** Use modern systems and software. If you have older technology you're making it easy for adversaries, especially if the technology faces the internet.

6. Takeaways

Key takeaways

1. APT groups are implicated in attacks targeting business information, research, government projects and individuals.
2. Healthcare has been a major focus in recent years.
3. During Covid-19 our institutions are more vulnerable, and effective protection means getting the basics right.
4. Healthcare leaders can establish visibility into cybersecurity and IT practices at their institutions to manage cyber risk.

Q&A

Appendices

A1. Pitfalls to avoid

A1.1 Pitfall to avoid: Lack of transparency

Governance groups and executive teams need visibility to make effective investment decisions. Warning signs:

- You don't understand your risk posture or how to change it.
- You don't understand how your organization measures up against leading practice or industry standards.
- You don't know what your cybersecurity team is doing.

A1.2 Pitfall to avoid: Lack of direction

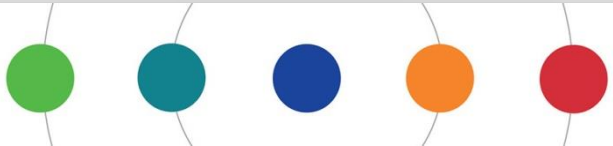
Do our teams know where they are supposed to be heading? Paraphrasing Steven Covey, successful institutions begin with the end in mind. Warning signs:

- You don't have a written information security strategy.
- You don't have a written implementation roadmap.
- You don't review implementation progress with executives or governance groups.

A1.3 Pitfall to avoid: Lack of process rigor

Cybersecurity is a battle between your organization and adversaries. Battles are won with discipline. Warning signs:

- You don't document information security policies and processes.
- You don't use project management to drive one-time activities.
- You don't identify and track meaningful maturity measures and performance metrics.



A1.4 Pitfall to avoid: Overconfidence

At all levels of the organization we have room to grow and learn from others: none of us know it all. Warning signs:

- You don't leverage outside experts.
- You don't benchmark against industry cybersecurity or information security standards.
- Your major initiatives don't solicit requirements from users.

A1.5 Summary: Pitfalls to avoid

Cybersecurity is a new technical discipline, but the same pitfalls apply as with information technology in general:

- Lack of visibility
- Lack of direction
- Lack of process rigor
- Overconfidence

A2. Approaches to consider

A2.1 What are we trying to do?

Before we can identify approaches, let's be clear what we're trying to accomplish and what we need to know:

1. We need to understand our cybersecurity risk, and know if there is something we should be doing now.
2. We need to control this risk through effective mechanisms, and understand what levers we have for this purpose.
3. We need to know if our efforts in these areas are effective.

A2.2 What can effective cybersecurity accomplish?

If implemented effectively, cybersecurity is a tool that enables executive leadership and governance groups to be able to manage a type of institutional risk. This means that we know:

1. The level of risk we are taking on (and any hotspots).
2. The levers we have to control that cybersecurity risk.
3. The performance of the cybersecurity capabilities that provide this visibility and implement those controls.

A2.3 Three approaches to consider

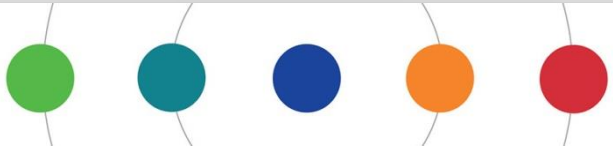
In practice, to understand and control our cybersecurity risk we will use approaches that provide good approximations:

1. **Measure governance, risk, and compliance (GRC):** Do we use policy to make decisions and manage exceptions?
2. **Measure IT hygiene:** How rigorous are our IT processes?
3. **Measure cybersecurity maturity:** How effective are we at the cybersecurity activities that we should be good at?

A2.4 Measure governance, risk, and compliance

Governance, risk, and compliance is a complex process and worthy of a talk of its own. If you're not doing it, talk to an expert:

1. Establish an information security GRC process, and use it to populate an ongoing information security risk register to share with leaders and governance groups.
2. Establish programs to mitigate these risks as appropriate.
3. Refresh the risk register and report it on a regular cadence.



A2.5 Measure your IT hygiene

IT hygiene is basically a measure of how consistently we perform IT activities. There's a range of measures that should be considered here:

- IT maturity against standards, (e.g. ITIL Service Management).
- Completeness of asset inventory or configuration database.
- Coverage of vulnerability scanning and patch management.

A2.6 Example measures of IT hygiene:

- How mature are we at ITIL Service Management?
- How accurate is our asset inventory? Metric: “things identified in the inventory” / “number of things on the network”
- How complete is our vulnerability scanning? Metric: “number of things scanned” / “number of things on the network”
- How complete is our patch management? Metric: “number of vulnerabilities patched” / “number of vulnerabilities found”

A2.7 Measure your cybersecurity maturity

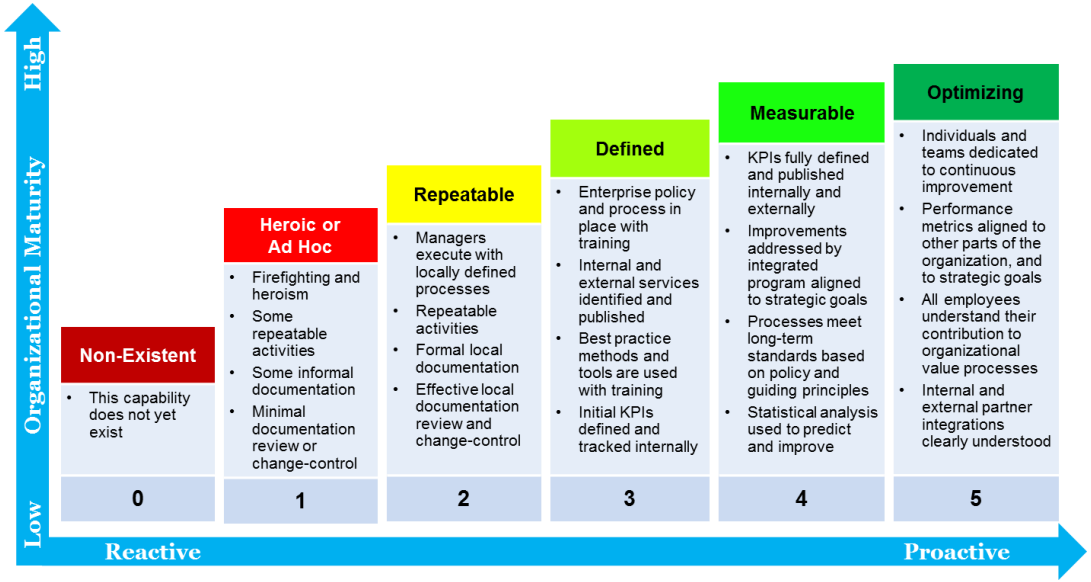
Maturity is a measure of how good we are at doing what we should be doing. Use outside experts to help provide assurance:

1. Establish a capability model (e.g. NIST CSF categories) and a measurement rubric (e.g. CMM 5-level score).
2. Establish current state and future target.
3. Establish program to get there, reporting on fixed cadence.

A2.8 Choose a capability model (e.g. NIST CSF):

Identify (ID)	Protect (PR)	Detect (DE)	Respond (RS)	Recover (RC)
Asset Management (ID.AM)	Access Control (PR.AC)	Anomalies and Events (DE.AE)	Response Planning (RS.RP)	Recovery Planning (RC.RP)
Business Environment (ID.BE)	Awareness and Training (PR.AT)	Security Continuous Monitoring (DE.CM)	Communications (RS.CO)	Improvements (RC.IM)
Governance (ID.GV)	Data Security (PR.DS)	Detection Processes (DE.DP)	Analysis (RS.AN)	Communications (RC.CO)
Risk Assessment (ID.RA)	Information Protection P&P (PR.IP)		Mitigation (RS.MI)	
Risk Management Strategy (ID.RM)	Maintenance (PR.MA)		Improvements (RS.IM)	
	Protective Technology (PR.PT)			

A2.9 Choose a maturity rubric (e.g. CMM levels):



A2.10 The first time you measure it won't be pretty

Identify	Protect	Detect	Respond	Recover
Asset Management 1.5	Access Control 1.5	Anomalies and Events 1.0	Response Planning 1.0	Recovery Planning 1.5
Business Environment 1.0	Awareness and Training 2.0	Security Continuous Monitoring 1.0	Communications 1.0	Improvements 1.0
Governance 1.5	Data Security 0.0	Detection Processes 0.5	Analysis 1.0	Communications 1.0
Risk Assessment 1.0	Information Protection P&P 1.0		Mitigation 1.0	
Risk Management Strategy 1.5	Maintenance 1.5		Improvements 0.5	
	Protective Technology 1.5			

A2.11 Establish a 1-year target:

Identify	Protect	Detect	Respond	Recover
Asset Management 1.7	Access Control 2.0	Anomalies and Events 2.0	Response Planning 2.0	Recovery Planning 2.0
Business Environment 2.0	Awareness and Training 2.5	Security Continuous Monitoring 1.7	Communications 2.0	Improvements 2.0
Governance 2.0	Data Security 1.4	Detection Processes 1.9	Analysis 2.3	Communications 2.5
Risk Assessment 1.7	Information Protection P&P 2.2		Mitigation 2.0	
Risk Management Strategy 2.0	Maintenance 2.3		Improvements 2.5	
	Protective Technology 1.6			

A2.12 Establish a 2-year target:

Identify	Protect	Detect	Respond	Recover
Asset Management 3.0	Access Control 3.0	Anomalies and Events 3.0	Response Planning 3.0	Recovery Planning 3.0
Business Environment 3.0	Awareness and Training 3.0	Security Continuous Monitoring 3.0	Communications 3.0	Improvements 3.0
Governance 3.0	Data Security 3.0	Detection Processes 3.0	Analysis 3.0	Communications 3.0
Risk Assessment 3.0	Information Protection P&P 3.0		Mitigation 3.0	
Risk Management Strategy 3.0	Maintenance 3.0		Improvements 3.0	
	Protective Technology 3.0			

Key: 0 0.5 1 1.5 2 2.5 3 3.5 4 4.5 5

A2.13 Measure progress until you reach your target: