CYBER THREAT LANDSCAPE
WHAT DOES IT MEAN TO MY ORGANIZATION?

ISACA Security Event

October 19, 2018

About your Speaker

Jeff Morgan

Manager

Security, Privacy & Risk Services

jeff.morgan@rsmus.com

https://www.linkedin.com/in/jeffrey-morgan-84ab7752/

- Over 7 years experience in information security, IT audit readiness support, and business process automation
- Originally from Cleveland Ohio – Go Browns?
- Worked within the government and at one of the big 4 accounting/consulting firms
- What I love about my job:
  - Working with clients to define strategies based on their current capabilities, threats, and business constraints
  - Helping clients implement strong foundational cyber capabilities to protect their business
- Career Highlight: Going to the White House

RSM

CYBER LANDSCAPE

Global Threat Environment

Current Threat Landscape

- Operates on a global scale
- Environment is constant and active 24/7
- Threat activity can be focused on an industry or more broadly
- Threat actors can be organized regionally or globally
- Threat actors are driven by motivation to achieve a defined objective
- Ability to scale their Tactics, Techniques, and Procedures (TTPs) as needed, based on their capabilities, to accomplish their objective

The Key Players

Nation States

Cyber Criminals

Hacktivists /Supporters

Lone Wolves

Insiders

Researchers

RSM

Primary Exploits Leveraged by Cyber Threats

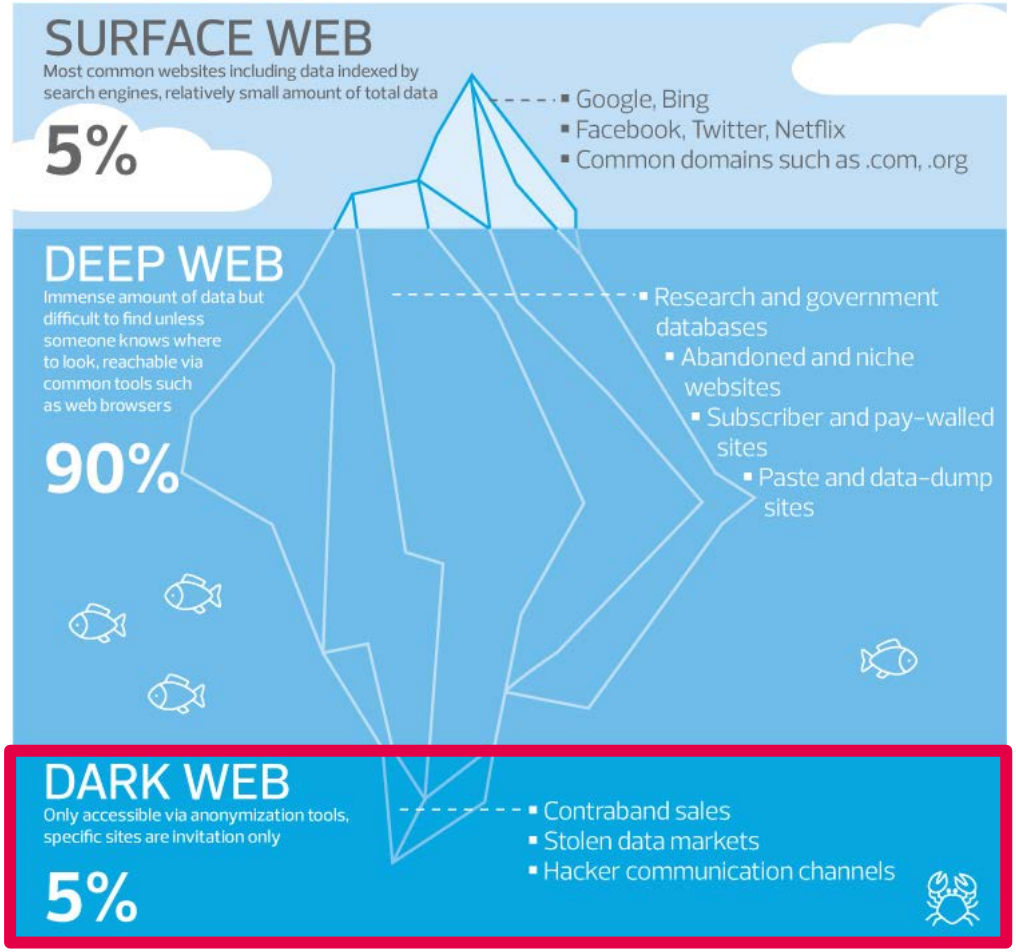
- **Hacking – Breaking through vulnerability and moving laterally**
  - Network penetration
  - Data leakage and theft
  - Social engineering

- **APT – "Uninvited Guest"**
  - Arrives into your network and stays there under the radar
  - Harvesting information over time
  - Typically not found with anti-virus software
  - Sophisticated

- **Malware – Code that is designed to do bad things**
  - Execution of malicious code on an infrastructure
  - Escalate unauthorized privileges
  - Shut down your network (DDOS)
  - Encrypt key data (Ransomware)

Operating in the Dark Web

- The Dark Web is the part of the web that requires anonymizing software to access
- It is built on the backbone of the internet, but requires specific software, configurations, or authorization to access
- The Dark Web is a subset of the Deep Web, which is unindexed by conventional search engines
- Consists of small, friend-to-friend peer-to-peer networks, as well as large, popular networks like Tor, Freenet, I2P, and Riffle operated by public organizations and individuals
- Within the Dark Web you will find:
  - Marketplaces
  - Forums
  - Pasta Sites
  - Search Engines/Wikis
  - Social Media/Chat Rooms



THREAT ACTORS

Nation States

Origin: US, China, Russia, North Korea, Syria

Target: Any other Nation State or Corporation that supports its ability to achieve is nationalistic agenda and goals.

Motive: Political, National Security, Economic

Objective: Influence political elections/positions, gain insight into military capabilities/objectives, acquire information to provide an economic advantage.

TTPs: Zero day and advanced capabilities not limited by financial or resource restrictions. These adversaries have the ability to access your network, move latterly to avoid detection and extract data covertly.

RSM

Cyber Criminals

Origin: Global with major hubs in Eastern Europe, Russia, and Asia

Target: Any entity that can be exploited to achieve their objectives.

Motive: Financial

Objective: Acquire data that can be sold for profit or control resources to conduct further attacks/mining activities.

TTPs: Advanced capabilities with the ability to acquire additionally capabilities on the open market. Quickly evolving toolset of malware loaders, trojans and ransomware that on par with some Nation States.

RSM

Hacktivists/Supporters

Origin: US, Europe, Russia and the Middle East

Target: Any Nation State, Religion or Corporation that they feel is conducting activities that are not aligned to their own beliefs.

Motive: Ideological, Disruption, Destruction

Objective: Target an entity in an attempt to harass and disrupt their ongoing ability to operate or to drive future change.

TTPs: Targeted capabilities to achieve their objective. Primarily have conducted DDoS attacks, web defacements and/or have conducted propaganda campaigns through social media.

RSM

Lone Wolves

Origin: Global with talent pools in Eastern Europe, Russia and the US

Target: Opportunistic based on motive or in alignment with a Cyber Criminal or Hacktivist objectives.

Motive: Financial or Recognition

Objective: Exploit an identified target based on the ability to financial gain from the attack or receive recognition in the hacking community or develop exploits to sell on the dark web.

TTPs: Capabilities vary greatly from simple social engineering and phishing campaigns to the development of sophisticated pieces of malware to leverage or sell as part of larger campaigns.

RSM

Insider Threat

Origin: Global

Target: Willing or unwilling participants

Motive: To enable the activities Nation States, Cyber Criminals, Hacktivists, and Lone Wolves.

Objective: Leverage the credentials and access of a willing or unwilling participant to bypass physical and network controls in order to achieve their desired objective.

TTPs: A willing insider may use their approved access to conduct their attack while an unwilling participant may have been comprised (knowingly or unknowingly) through a phishing campaign or watering hole attack.

RSM

Researchers

Origin: Global with a focus on US and Europe (White Hats)

Target: Any potential vulnerability in an organization.

Motive: Curiosity, Recognition, Financial

Objective: Identify vulnerabilities because it is a passion of theirs and they are looking for the recognition from their work and the potential financial gains associated with bug bounty programs.

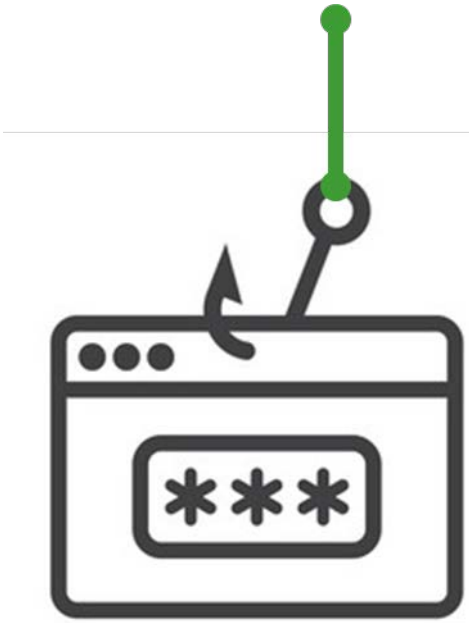
TTPs: Leverage various TTPs in an effort to evaluate the security posture of an organization in an effort to identify potential vulnerabilities that could be exploited by future threat actor.

RSM

Why are threats still successful – Human Element

Phishing by the numbers

- 92.4% of malware is delivered via email
- 30% of phishing messages get opened by targeted users
- 12% of those users click on the malicious attachment or link
- Shift away from malicious attachments to URLs
  - 2017 – 3 of 4 emails delivered malware via an attachment
  - Q1 2018 – malicious URLs outnumbered attachments 4-1
- Most common disguise for distributing malware
  - Bill / invoice (15.9%)
  - Email delivery failure (15.3%)
  - Legal / law enforcement (13.2%)
  - Scanned document (11.5%)
  - Package delivery (3.9%)



- Average phishing attack can cost a mid-size company nearly $1.6 million
- Losses associated with Business Email Compromises have double in the past year and the threat actor is averaging $130 thousand per successful attack
- 95% of all attacks on enterprise networks are the result of successful spear phishing

RSM

Why are threats still successful – Technology

- Open Web Application Security Project (OWASP) conducts an annual survey to identify the top 10 vulnerabilities to applications
- Over the years the list has remained fairly consistent allowing the threats to enhance their tools and focus them against the same vulnerabilities

	OWASP Top 10 - 2013	OWASP Top 10 - 2017
1	Injection	Injection
2	Broken Authentication/Session Management	Broken Authentication/Session Management
3	Cross-Site Scripting (XSS)	Sensitive Data Exposure
4	Insecure Direct Object Reference	XML External Entities (XXE)
5	Security Misconfiguration	Broken Access Control (items 4+7 merged)
6	Sensitive Data Exposure	Security Misconfiguration
7	Missing Function Level Access Control	Cross-Site Scripting (XSS)
8	Cross-Site Request Forgery (CSRF)	Insecure Deserialization
9	Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities
10	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring

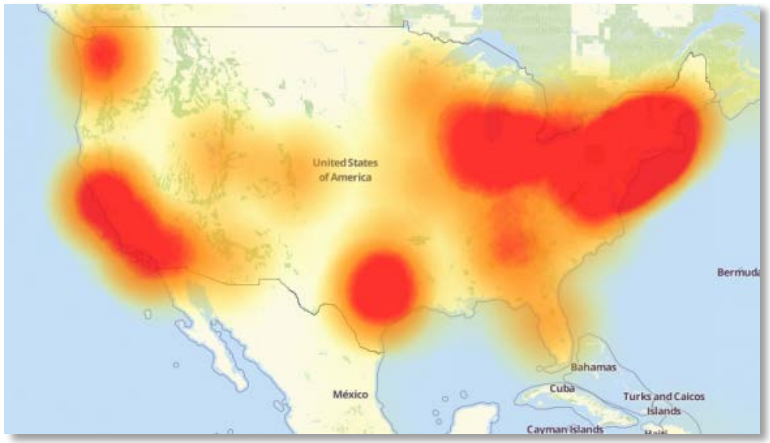
Present in 2013 and 2017 | New in 2017

RSM

EMERGING THREAT ACTIVITY

IoT Malware – Disrupting Global Business

- In 2017 there were at least 8.4 billion IoT devices
- Many of these devices are easy targets do to limited oversight, outdated security features, and default security settings (passwords)
- It used to be easy to remove malware on IoT devices because they could just be unplugged, however new variants live in the devices directory and can reinstall on a reboot
- These devices are typically controlled as large botnets in order to conduct:
  - Distributed Denial of Service (DDoS) attack - Mirai botnet made the internet inaccessible for much of the eastern US in 2016 by controlling IoT devices that had default credentials in place
  - Cryptocurrency Mining – Can create performance issues in the devices controlled and experts say that 15,000 internet-connected devices could be hacked to mine $1,000 of cryptocurrency in just 4 days
- New IoT Malware, the Reaper, has already infected an estimated one million organizations and is dubbed the “cyber-storm that could take down the Internet.”
- Reaper, unlike Mirai, does more than just use default credentials, it is set up to exploit known security vulnerabilities on IoT devices

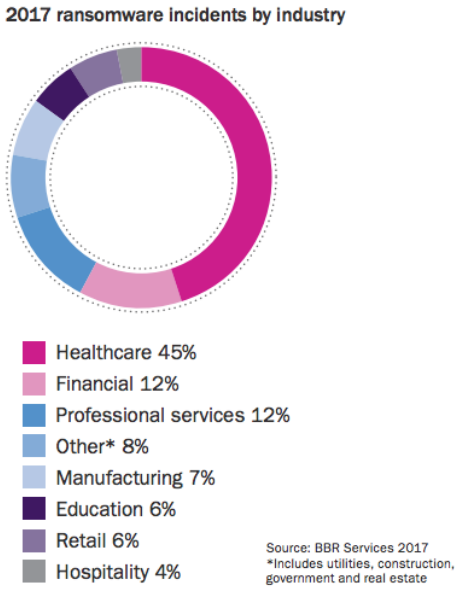


Outages caused by the Mirai attack on Dyn

RSM

Ransomware – Bringing Operations to a Standstill

- Type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid
- First prominent attacks began in 2005, but have grown exponentially since 2012
- The average cost per ransomware attack to businesses was $133,000 in 2017
- Attackers are typically requesting bitcoin or other forms of cryptocurrency as payment to unlock files
- Attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment
- Additionally, there are currently 3 million endpoints with RDP connections exposed to the Internet that threats can exploit to manually deploy their malware
- WannaCry was a gamechanger by spreading automatically through the internet an infecting more than 230,000 computers in 150 countries
- After getting hit by the SamSam ransomware in March 2018, Atlanta, Georgia, has spent more than $5 million rebuilding its computer network, including spending nearly $3 million hiring emergency consultants and crisis managers.



Cyber Propaganda – Diminishing Brand Value

- Defined: The use of information technologies to manipulate an event or influence public perception toward a certain point of view
- More commonly referred to as “Fake News”
- Can be used to sway public opinion – cause negative sentiment against you and positive sentiment for your competitor
- Paid services are used to buy comments, likes, retweets, etc. and even campaigns to manipulate online polls
- Objective of an attack is to impact your brand
- Can also be leveraged to organize demonstrations against your organization
- Social media sentiment analysis is one of the best ways to understand how your brand is being perceived in the market

STEPS TO TAKE

Training & Awareness – Enhancing security through information and knowledge

- Should be more than a one time event
  - Yearly training, monthly refreshers/tips, periodic alerts
- Tailored for target audiences (Executives, Operations, IT, etc.)
- Incorporate relevant material based on the current threats to your organization
- Aligned to the industry you operate in and the technologies you use
- Should address any relevant laws or regulations
- Results should be tracked and metrics gathered for reporting
- Should always include the basic elements of security:
  - Physical security best practices
  - Password requirements and best practices
  - Phishing awareness
  - Social engineering awareness
- Training materials should be evaluated periodically and updated to stay relevant
- Training materials should not just tell you what to be aware of, but what to do in the event of an incident

“Make Passwords Great Again”

Incident Response
– Limiting the impact of an incident

- **Have a documented plan in place!!!**
- Create a team with representation from across the organization
- Identify and document which systems are critical to the organization
- Identify external parties that you may need to communicate with
- Integrate with your public relations teams and develop internal and external communication channels
- Define scenarios and develop runbooks based on the highest risks to your organization
- Develop a checklist to guide your incident response plan
- Make sure the activities that are being conducted align to any regulatory and legal obligations you may have
- Test, review and update

RSM

Vulnerability & Patch Management – Proactively fix known issues before they can be exploited

- Conduct regular scanning and include everything that touches your network
- Define accountable and actionable policies and procedures
- Monitor vulnerabilities from identification through completion
- Stay current with your asset inventory
- Document the security controls you have in place across your environment
- Compare reported vulnerabilities against your asset inventory and control lists
- Identify and classify risks to support the prioritization of remediation efforts
- Apply patches to the most critical assets in a timely fashion
- Develop metrics to support decision making
- Standardize the process to support consistent activities
- Consider push updates to confirm the patch is being applied
- Test/QA to make sure there are no long term issues

RSM

Threat Intelligence – Identify if you have been compromised without knowing

- Perform due diligence sweeps across open and closed sources for your data
- If data is found, determine source and potential root cause of the leak
- If accounts and passwords are found, inform users and require them to update their passwords
- Perform Dark Web investigations on an ad-hoc basis depending on your sector and industry to determine if there are any emerging threats to be concerned about
- Conduct intelligence briefings and C-suite level reporting to keep executives informed
- Build out internal threat intelligence capabilities to improve overall cybersecurity strategy and determine exposure risks
- Incorporate information acquired for potential threats into the training and awareness program through bulletins and alerts
- Update your controls environment as needed based on new and emerging threats

QUESTIONS

THANK YOU
FOR YOUR TIME
AND ATTENTION

RSM US LLP
100 South Ashley Dr. Suite 1770
Tampa, FL 33602

+1 800 274 3978
www.rsmus.com

RSM