**INTRODUCTION/TRANSITION FROM DAVID McDowell:**

**Good afternoon, I am Mark Sadler, and I am a Divisional Vice President with Great American’s Cyber Risk Division**

* In my role, I work with a number of policyholders in the small to middle market or SME space facing cyber incidents – this afternoon we will take a look at some of the common events we see and some suggestions for mitigation.
* While a cyber incident is a serious event for any enterprise, it can threaten the existence of SMEs.
* Of the cyber incidents I see, the most frequent are ransomware attacks and business email compromise events.

**S1/RANSOMWARE – FREQUENCY AND SEVERITY:**

**Frequency:**

* There is a ransomware victim every 10 seconds
* There have been 4,000 attacks daily since 2017
* Cyber insurers and consultants report that 35-40% of new incidents involve ransomware
* One carrier reported a 950% increase in ransomware claims over the last three years.

**Severity:**

* The Global cost of ransomware attacks including remediation expenses has been estimated as high as $20B.
* Average ransom payments in have been estimated as high as $350M by a leading cryptocurrency data firm.
* Since 2017, the average ransom demand has increased from $15K to $175K and seven figure or higher demands are not uncommon.
* A report by Coveware placed the average ransom payment for Q1 2021 at $220,298
* DISCUSS 2-track approach > restoration /engagement
* However, doxing aside, the presence of viable backups is a key variable in determining severity and available options in addressing an attack.

**Attack Vector:**

* The most common attack vectors that we are seeing are *Phishing* and *Exploitation* of vulnerable RDP ports.
* These trends as have accelerated with the increase of remote work starting in 2020.
* Another common attack vector has been *software vulnerabilities*. During Q1 2021 the most common vulnerabilities exploited involved VPNs.

**Sectors Impacted:**

* Education – local school districts and colleges.
* Healthcare – we have had some involved in delivery of CV19 therapy and treatment.
* Manufacturing
* Professional Services – accountants during tax season.
* Each of these groups are particularly impacted by a shutdown. Examples – school district during holiday break or accountants during tax season.

S2/**RANSOMWARE – CLAIM TRENDS**

We have seen two primary types of attacks, ***Targeted Attacks*** and ***Ransomware as a Service***. Generally,

**Targeted Attacks** involve a higher level of sophistication and these groups tend to research and select their targets more carefully.

* They generally spend time in an environment moving laterally then conducting reconnaissance. It is not uncommon to discover that they have been present in an environment for weeks or months prior to the actual ransomware attack.
* The ransomware variants tend to be more sophisticated in targeted attacks – more recently, we have seen a lot of involvement with sodinokibi, maze, conti and zeppelin.
* The ransoms demanded by the Targeted Attackers is generally much higher.
* There are also often exploits in addition to the ransomware attack involved, such as exfiltration of data or financial fraud.
* One positive is that there is that we have seen fewer instances of data corruption with attacks by targeted groups.

**Ransomware as a Service**, in our experience, involves less sophisticated actors.

It involves an arrangement where “developers” who buy or develop the malware advertise and recruit “affiliates.” The affiliates deploy the ransomware and negotiate the ransom, and the developers get a cut of the proceeds, typically 30-40%.

We have seen more instances of attempted double extortion or corrupted data with RaaS actors and generally find that the technical ability of these actors is far less than we see with targeted attacks.

**Doxing,** or the practice of demanding a ransom to prevent disclosure of stolen data onto “shaming sites” or attempted monetization on the dark web became common place in 2020 and happened in a majority of the cases I have seen in the last 6-9 months. Coveware reported in its recent quarterly report that 77% of attacks involved a threat to leak exfiltrated data.

Even in cases where viable backups exist you may have to deal with a doxing threat. In an interesting variation on this trend, I also read recently of a threat group that published a transcript of ransom negotiations. There have also been cases where threat groups have called or otherwise contacted victims directly in an effort to pressure a ransom payment.

**Attacks Involving Third Party Data Aggregators**: during 2020, there were some high-profile attacks against data aggregators, that impacted local policyholders in different ways. One of the most well know attacks involved Blackbaud, a large cloud service provider.

Although policyholders were not involved in the ransomware attack itself, they were required to provide notice to individuals and regulators and in some cases suffered contingent business interruption losses.

S3/**RANSOMWARE – COMMON COVERAGES IMPLICATED**

* Extortion – Requires Prior Approval
* Legal / Breach Coach
* Forensics – which include incident response and ransom negotiations.
* Notification
* Public Relations – which is especially important in cases involving doxing.
* Restoration – Often required after decryption / deployment of decryption tool / corrupted systems.
* Business Interruption / Contingent Business Interruption

S5/**BUSINESS EMAIL COMPROMISE**

* Business email compromise includes unauthorized access to an organization’s email system, in an attempt to commit fraud and/or exfiltrate data. From a frequency standpoint, these incidents comprise another 35-40% of the incidents reported.
* In recent years, this threat has been increased with the migration of on-premises email servers to cloud—based solutions such as Microsoft Office365.
* According to the FBI’s Internet Computer Complaint Center or “IC3” in 2020 they received 19,369 Business Email Compromise of Email Account Compromise complaints with adjusted losses totaling over $1.8B.
* The losses are generally accomplished through phishing or other social engineering attacks or computer intrusion techniques.
* The common motive in the most common BEC attacks is financial fraud. However, a leading forensic firm reported that almost half of the BEC cases they investigated also involved data exfiltration.

S6/**BUSINESS EMAIL COMPROMISE – COMMON ATTACKS**

We have seen several variations of business email compromise attacks:

* A spoofed email that from a senior executive directing the recipient to wire funds to a third party on an urgent basis.
* A different version of this attack involves an email from a senior executive asking the recipient to purchase gift cards and provide the gift card numbers often for a purported corporate event or an important client.
* Another well-known attack starts with an email from a known vendor or employee requesting to change their account payment details. This email may come from the authentic email address associated with the vendor/employee (because the fraudster has infiltrated an email account), or from an email account that is so similar to the authentic address that it is easy to miss the difference.
* We often see bad actors using "email auto-forwarding rules" to forward or redirect an incoming email to another address. This allows them to receive copies of incoming emails without having to log into an account each day -- and risk triggering a security warning for a suspicious login.

S7/**RANSOMWARE – COMMON COVERAGES IMPLICATED**

* Legal / Breach Coach
* Forensics – for cases involving infiltration of a system and often involves data mining of data stored in email boxes.
* Notification
* Social engineering coverage such as coverage for fraudulently induced transfers if available.

S8 AND S9/**MITIGATON STRATEGIES**

* Prompt Notice to Breach Coach and Insurer.
* Do not contact the attacker in ransomware matters.
* Do not wipe or restore drives before consulting forensics.
* Prompt deployment of software patches.
* Manage open ports.
* Require complex passwords and multi-factor authentication where possible.
* Employee training to identify phishing emails and suspicious links.
* Voice verification of account changes and wire instructions

**CLOSE**: **Thank you for the opportunity to present this information. I am happy to address any questions.**