Division *of*
Risk Management

Transcript for Risk Symposium Presentation: Cyber Threats and Coverage

Date: April 23, 2026

Speaker: Jonathan Stutz, Moreton & Company

Introduction & Speaker Background

Speaker (Rachel): John has an official bio, but I'll give my own bio. John is the broker—he is with Moreton & Company—and he is the best broker ever, and we love him so much. He has over 20 years in the industry. He works on the most complex, the craziest stuff. He handles all of our insurance, he also does cyber—which is not through Risk—he also does all the crazy stuff like, *"Hey John, the state just bought a magnesium plant out of bankruptcy, now what?"* or *"Hey John, the university just bought the two most adorable Highland cows, now what?"*

So, John does all the crazy, all the complicated, and we love him. If there are things outside of what Risk can cover, John should be your best friend. So, John's the best, that's your bio, and we're going to let him cover cyber threats and coverage.

Opening Remarks & Icebreaker Jokes

Jonathan Stutz: Thanks, Rachel. I don't know where to go from that—I should probably just sit down! Well, it's great to be with you. Good morning! Good morning to those here in the room, good morning to those online.

I'll start out with a couple of jokes here, we'll see how they land.

I used to have a joke I told about **UDP protocol**, but I could never tell if they got it.

(Laughter from audience)

If you understood that joke, you probably don't belong in this presentation, because I didn't understand this joke! It's pretty technical.

We're going to keep this presentation a little more dumbed down, a little more applicable to everybody. So here are some jokes for all of us here:

1. **Did you hear about the cybercriminals that got away?** They ransom-ware.
2. **What is a hacker's favorite season?** Phishing season (with a P-H).

Those jokes were ph-fat!

Evolution of Cyber Liability Over 19 Years

Jonathan Stutz: Good to be with you here. As Rachel mentioned, I am the broker for the state for all different lines of coverage, but I have to tell you: **cyber liability is my absolute favorite thing to talk about.** It's my favorite thing to give presentations on. I just think it's dynamic.

I was looking yesterday at when I gave my first cyber liability presentation—it was 19 years ago. 19 years ago, when we were talking about cyber threats and coverage, we were really talking about **internet media liability** stuff. So, if you had a webpage and you posted a photo or somebody's likeness/image on there and you didn't have the rights to it, that's what cyber insurance was really concerned about at the time.

That's really not as much what cyber insurers are concerned about today, although when Rachel, Brian, and I were in London, we met with the state's cyber insurance company and asked: *"What are you guys worried about right now?"*

And they said, *"Well, you know, we are worried about ransomware, phishing attacks, and social engineering, but the thing we're starting to see claims on is media liability stuff on social media—people utilizing songs specifically that they don't have the rights to."* A lot of people, when they post on social media, just put a song up in the background of their video or TikTok without having the rights to it. So in your organizations, make sure that if you're utilizing any type of music in your social media, you have the rights to utilize it, because the music companies are coming after those who violate that.

Ransomware: The "Monday Morning" Scenario

Jonathan Stutz: Okay, Monday morning. You come into the office, you open up your computer, and it looks like this:

**** Ransomware Screen Displayed:**** *"Ooops, your files have been encrypted!"* (WannaCry Ransomware Example)

Hopefully none of you have experienced this. This specific one is called **WannaCry**, and there's a specific reason why people who get this want to cry!

Ransomware: If you see this screen, guess what? The bad guys have already been in your computer system for weeks, months, sometimes even years.

Does anyone know the reason why they wait so long before they trigger the ransomware?

Audience Member: Get your data.

Jonathan Stutz: Yeah! They're trying to get your data. They're trying to find the really important, valuable data to identify it, and they're also trying to get through all of the security controls you may have in place across your networks and systems so that they're able to encrypt *everything*.

Case Study: The $5.4M Ransom Demand

Jonathan Stutz: One example: About 10 years ago, I had a fairly large client. We were meeting with an insurance underwriter, and I said to this client, *"You know what? You guys should really be buying business interruption coverage with your cyber policy."* It was offered for about 10% additional premium.
My client said, *"You know what, that's never going to happen to us."* (Which is a total jinx when you say that!) He said, *"We have computer systems in the US, Latin America, Europe... if any of our computers get compromised in this country, we can pivot to a different continent and handle our business seamlessly."* I said, *"Okay, I offered."*

Well, less than a year after that conversation, it hits the news and I get a call: They had a ransomware attack. And guess what? They locked down the US, they locked down Latin America, they locked down Europe. They had been in their system for a long time, and they locked down their backups. A lot of people say, *"Well, we can restore from backups."* Well, the bad guys try to encrypt and get access to the backups as well so you can't restore from them. That's how they get their money, usually demanding payment in Bitcoin.

The really interesting thing about these ransomware criminals is they have good customer service! On this screen, there's a button that says "Contact Us." If you click on that, it actually goes to somebody who says, "How can I help you? Do you need help buying Bitcoin? Sure, I can help you with that!" Meanwhile, the clock keeps ticking down to when they will erase all of your data unless you pay.

How Bad Actors Determine Ransom Amounts

Jonathan Stutz: How often do you think ransoms get paid with ransomware? All the time! Why do you think people pay these ransoms?

Audience Member: Urgency of the clock, and whatever they can lose.

Jonathan Stutz: Yeah! The bad guys go after the really valuable data and say, *"I've got your really valuable data here, and if you don't pay the ransom, I'm going to release it on the dark web so all the criminals in the*

world get access to your sensitive, proprietary data, employee info, and customer info." A lot of organizations realize that taking that risk would destroy their business, so they feel forced to pay.

With that client ancillary to ours that had a ransomware attack, the Bitcoin demand was $5.4 million. They clicked the customer service button and said, *"Oof, we don't have $5.4 million, can we pay you $100 grand?"* The bad guys responded back with an email containing an attachment: *"Is this your financial statement?"* (It wasn't a publicly traded company). Because they had been in the system, they found their private financial statement and said, *"We see that you have $5.4 million in cash. We know you can pay this!"*

Ransomware Trends & Targeted Industries

Jonathan Stutz: As time has gone on, ransomware situations have become much more sophisticated and dangerous. That has led to insurance premiums going up significantly over the last few years (especially in 2022 and 2023).

Ransomware Attacks by Month 2021-2026 (Source: Cyble)
- Shows exponential increases in attack volume year-over-year.

Most Targeted Industries by Ransomware Attacks:

1. Professional Services (20.4%)
2. Consumer Services (12.8%)
3. **Public Sector (10.2%)**
4. Materials (9.7%)
5. Healthcare (7.7%)
6. Financial Services (6.6%)

The bad guys target public sector employees and organizations because the data and money held by the public sector is substantial.

Root Causes of Ransomware Attacks

Jonathan Stutz: When we look at root causes (data from Sophos Ransomware Report, April 2024):

- **Exploited Vulnerability:** ~32-35%
- **Social Engineering (61% combined):**
    - Compromised Credentials (~28%)
    - Malicious Email (~24%)
    - Phishing (~12%)
- **Brute Force Attack / Downloads (~3-5%)**

Over 61% comes from social engineering, compromised credentials, malicious emails, and phishing.

Social Engineering Demonstration (Video Clip)

Jonathan Stutz: Last week I attended a training with an FBI representative who showed a 2-minute video on social engineering. It was so impactful and insightful that I wanted to share it with you today:

[11:08 – Video Clip Summary: Real Future / Fusion.net]

- **Title:** Watch This Hacker Break Into My Cell Phone Account in 2 Minutes
- **Participants:** Reporter & Jessica Clark (Social Engineer Hacker at DEF CON / Social Engineer Village).
- **Method:** "Vishing" (Voice Solicitation) + Call Spoofing + Sound Effects.
- **Execution:** Jessica spoofs the reporter's phone number and calls his mobile carrier. She plays a YouTube audio clip of a baby crying loudly in the background. She pretends to be his stressed wife, claiming they are applying for a loan and she urgently needs access/email setup on the account.
- **Result:** In under 30 seconds, using the reporter's girlfriend's name, a fake SSN, and a crying baby sound effect, she gains full access to his cell phone account, adds herself to the account, and changes his password to "Jess."

Jonathan Stutz: Crazy, right?

Q&A Session: Ransomware & Dark Web Dynamics

Moderator: We have a question from online.

Online Question: *"How do you know that they won't put the data out on the dark web anyway?"*

Jonathan Stutz: That's a fair question! Going back to ransomware, there's an interesting dynamic: If they end up putting that data on the dark web anyway, they lose credibility. People will stop paying ransoms if the ransom agreement doesn't work out after you pay the money. So, bad actors are actually incentivized to "keep their word" in a twisted way—providing the decryption key and not leaking data once paid. That's their business model.

Now, there are criminals who don't care and will leak it anyway. Insurance companies actually maintain a log of who the "good" criminals are versus the "bad" criminals! They advise insureds during ransomware events on whether specific threat actor groups reliably honor their agreements.

Audience Question: If these groups are able to maintain a reputation and have customer service, why aren't they prosecuted?

Jonathan Stutz: It's crazy that they have email addresses and customer service, yet federal agencies struggle to track them down. A lot of them are state-sponsored or located in foreign countries outside US jurisdiction, making prosecution extremely difficult. Furthermore, there is now Ransomware-as-a-Service (RaaS) sold on the dark web, allowing almost anyone to buy malware code and run their own ransomware business.

Audience Member Comment: I used to work in fraud. In some Eastern European countries/neighborhoods, hackers literally put tally marks on their windows showing how many accounts they've compromised as neighborhood bragging rights. It's praised rather than prosecuted.

Social Engineering Prevention & Best Practices

What Organizations Can Do:

1. **Simulated Phishing & Training:** Essential practice to build muscle memory (even if employees find extra training modules annoying when they fail a test!).
2. **Multi-Factor Authentication (MFA):** Another layer of friction, but crucial protection.
3. **Advanced Email Security / Filtering:** External email banners/warnings.
4. **Secure Email Gateways:** Automated scanning for malware attachments.
5. **Culture of Security:** Taking extra seconds to inspect incoming emails carefully.

What You Can Do Personally:

- **Verify, Verify, Verify:** We see many social engineering/funds transfer fraud claims where an email claims, "Hey, I'm a vendor, we changed our bank account, please send payment here." Always verify bank change requests via a known, trusted phone number—never call the phone number listed inside the suspicious email requesting the change.
- **Follow Established Procedures:** Do not let artificial urgency or emotional appeals (like the crying baby in the video) bypass verification protocols.
- **Be Careful with Personal Info on Social Media:** People post details like birthdays, children's names, elementary schools, pet names, etc.—all of which are common security questions or password recovery answers!
- **Don't Click on Links:** Especially links in unexpected emails or text messages.

State of Utah Cyber Insurance Programs

The Division of Risk Management structures cyber coverage across three main buckets:

DTS Program (State Agencies)	School District Program	Higher Ed Program

• Covers all State Agencies where DTS handles Cyber Security. • $5M Aggregate Limit • Insurer: Lloyds of London • Claim Contacts: Phil Bates (DTS CISO) & Jonathan Stutz (Moreton)	• Covers all School Districts in Group Program (except 1 that opted out). • $5M Agg / $2M per SD • Insurer: AXA XL • Claim Contacts: Troy Jessup (UEN) & Jonathan Stutz (Moreton)	• Individual University Policies purchased by each institution. • Insurers: Beazley, Travelers, HCC, Boxx • Claim Contact: Jonathan Stutz (Moreton)

What Cyber Insurance Covers & Incident Response

Cyber Insurance Extensions:

- 1st Party & 3rd Party Coverage
- Regulatory & Public Relations Support
- Ransomware / Extortion / Business Interruption
- Social Engineering / Funds Transfer Fraud

Services Included with Policy Purchase:

- Claims Hotline
- Privacy Attorney Resources (Breach Counsel)
- Forensic IT Resources
- Notification & Credit Monitoring Services
- ID Theft Resolution Case Managers
- Public Relations / Crisis Management

Incident Response Timeline ("Friday Afternoon")

Discovery of Event	Evaluation	Short-Term Crisis	Long-Term Consequences
• Theft / Loss of Data	• Forensic Investigation & Legal Review	• Notification / Credit • Public Relations	• Class-Action Lawsuits • Regulatory Fines • Reputational Damage • Income Loss

Crucial Takeaway on Reporting Timeframes:

If there is a breach or fund transfer fraud incident, notify Risk/DTS immediately.

- **Within 24 Hours:** Fraudulent fund transfers can usually be frozen and recovered if reported within 24 hours.
- **After 24 Hours:** Recovery becomes exponentially harder as time passes.

Conclusion & Final Q&A

Jonathan Stutz: I sped through that last part, but I wanted to leave a couple of minutes for any additional questions regarding cyber programs.

(No further questions raised)

Jonathan Stutz: All right, we did it! Thank you very much!