Lions and Tigers and Bears, Oh My! What to do for a Data Breach

Presented By:

Kevin M. Scott
Greenberg Traurig, LLP

Scott Tenenbaum
Axis Capital

Billy M. Evans Jr.
Kivu Consulting

MAY 12, 2023

GT GreenbergTraurig

Today's Presenters

Scott Tenenbaum

Head,
North American Cyberclaims
Axis Capital
New York, NY

Kevin M. Scott

Shareholder,
U.S. Data, Privacy & Cybersecurity
Practice, Greenberg Traurig
Chicago, IL

Billy M. Evans, Jr.

Chief Operating Officer,
Kivu Consulting
San Antonio, TX

GT GreenbergTraurig

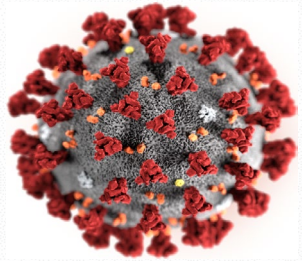
Your Organization Will Survive a Breach

- **Timing:** How quickly did you respond?
- **Communication:** How well did you communicate with stakeholders, regulators, and the public?

GT GreenbergTraurig

Since March 2020, Why an Increased Cyber Risk?

- Transition of workforce to remote due to COVID-19
- Distracted workforce
- Heightened emotions/fears
- Increased ingress traffic from external sources
- Increase in number of endpoints with decreased control and visibility
- Shadow IT efforts by employees



Why Should My Organization Be Prepared?

$4.62 million

Average total cost of a ransomware breach, more expensive than the average data breach ($4.24 million)

2X

Ransomware doubled in frequency in 2021, appearing in 10% of all reported data breaches

$211,529

Average ransom payment in Q1 2022

77%

Of ransomware cases use data exfiltration as a tactic

Aside from cost, there are many other potential consequences of a ransomware attack, including legal ramifications and reputational damage.

GT GreenbergTraurig

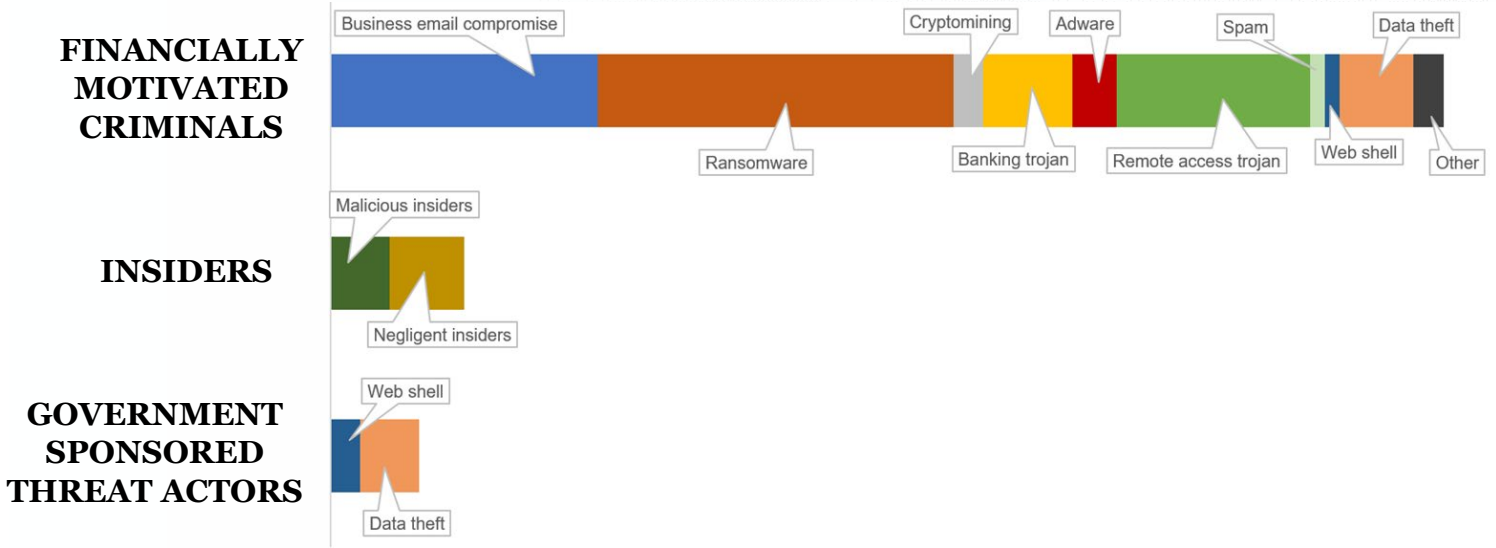
Data Security Trends

- Ransomware is King
  - Increase in attacks 36 months ago
  - FBI received 2,385 reports in 2022, a 36% year-over-year decrease however, ransomware totals increased
- Business Email Compromise for Wire Transfer Fraud
  - 2022 - $2.74 billion in reported, exposed losses (billion with a B!), per the FBI
  - 10% increase in attacks in 2022, a year-over-year increase

GT GreenbergTraurig

Anatomy of the Attack

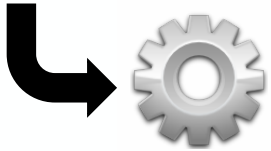
Based on our most recent data:



GT GreenbergTraurig

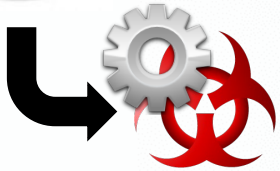
Anatomy of the Attack

1 Initial Entry



2 Lateral Movement and Recon/Backup Destruction

3 Data Exfiltration



4 Ransomware Deployment

****Initial Entry****

- Malware Infection
- Scan-and-Exploit
- Credential Abuse

GT GreenbergTraurig

Are These Attacks Preventable?

Malware Infection

Endpoint and Network Detection

Scan-and-Exploit

Patch

Credential Abuse

Multi-Factor Authentication

GT GreenbergTraurig

Ransomware "Trends"

- Increase in number of threat actors
- Franchising ransomware
- Increase in monetary demands
- Increase in data access/exfiltration
- Name and Shame sites
- Contacting victims

WHERE ARE WE NOW?
Currently, there is an uptick in the market with attackers purchasing more expensive equipment to achieve their targeting goals of "hard to access" companies

FOOD FOR THOUGHT:
Increased IT security spending = lower risk of attack = increased expense to attackers = increased barrier = **fewer attackers**

GT GreenbergTraurig

Responding to a Ransomware Attack

Identify the following early on:

- What happened?
- Is the incident ongoing? (If so, first priority is cutting off any harm)
- Can you restore from back-ups? How long will that take?
- What information was potentially exposed?
- How many people could be impacted? Where do the impacted individuals live?
- Should you contact the threat actor?

- Is the company subject to any special regulations based on industry type?
- Does the company have any third-party notification obligations?
- Do you have a communications strategy? Media? Employees? Individuals? Regulators? Law enforcement?
- Does the company have cyber insurance?
- Has a forensic investigator been retained?
- Does the company have access to a crypto wallet to make the payment?
- Does the company have time/resources to restore post receipt of decryption key?

GT GreenbergTraurig

Threat Actor Negotiations

- Vendors can manage negotiations
- Understand your threat actor (e.g., will they negotiate?)
- They have done their homework (and may know your financials)
- Honor among thieves?

PYSA

Hi Company,

Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:
Vankibrryy@onionmail.org
Frankbankss@onionmail.org
Kymanipitman@protonmail.com

Also, be aware that we downloaded files from your servers and in case of non-payment we will be forced to upload them on our website, and if necessary, we will sell them on the darknet.
Check out our website, we just posted there new updates for our partners: http://pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad.onion/

GT GreenbergTraurig

Threat Actor Negotiations

2021-02-11 13:10:39 SUPPORT

Hello, this is XingLocker Team. Please, introduce yourself (Company name and your position) and we'll provide all necessary information. Sometimes our staff is busy, but we will reply as soon as possible. Be in touch, thank you. For your attention. We have more than 100 GB of this kind of data, and huge part is high privacy level.

2021-02-12 13:00:57 DGHC01

Where do we go from here?

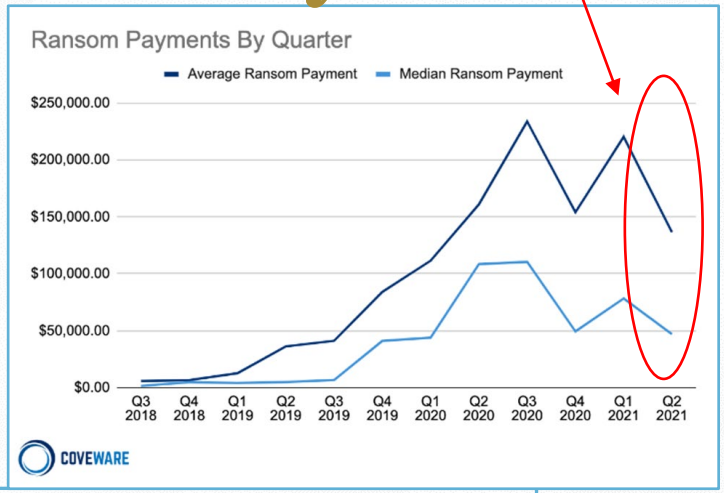
2021-02-12 13:01:46 SUPPORT

You are here because of your network penetration. To get a decryption tool and to avoid publication of your data you have to pay a ransom. The amount for full decryption and permanent deletion of your data is 10 Million dollars. Publication of full dump will cause terrible damage for your company. We can send one free unlock for you - you can decrypt 1 file to be sure we are able to decrypt all your network. Please, inform your management about the situation and show them the proofs. We are here to negotiate and waiting for your offer.

GT GreenbergTraurig

Ransom: To Pay or Not To Pay?

- Pros v. Cons
- Back-ups
- How do you feel about paying a criminal?
- Will you get your data back?
- Time = Money



Where are we today?

- Because of stricter insurance standards, there is potential for new regulation:
  - Proposed laws against making ransom payments
  - Mandatory federal reporting of ransom payment
    - Provide incident data – government grasps the issue = ⇩ victim payments

GT GreenbergTraurig

Office of Foreign Assets Control (OFAC) Sanctions and Guidance – October 1, 2020

- Sanctioning began in December 2016 and will continue on threat actors and those who assist, sponsor, or provide financial, material, or technology support relating to ransom attacks.
- Ransom payments not only encourage the behavior, but they can attribute to potential threats to U.S. national security and foreign policy objectives.
  - Payments **do not** guarantee restored access
- Payments May Violate OFAC Regulations per IEEPA and/or the TWEA
  - Civil Penalties
- Implementation of risk-based compliance is encouraged
  - Banks, cyber insurers, forensic investigators/incident response – may have obligations under FinCEN
- Victims should contact OFAC immediately if involves a sanctions nexus

Where are they now?
Increased pressure on foreign governments to stop condoning cyber crime = threat actors facing consequences in their own countries

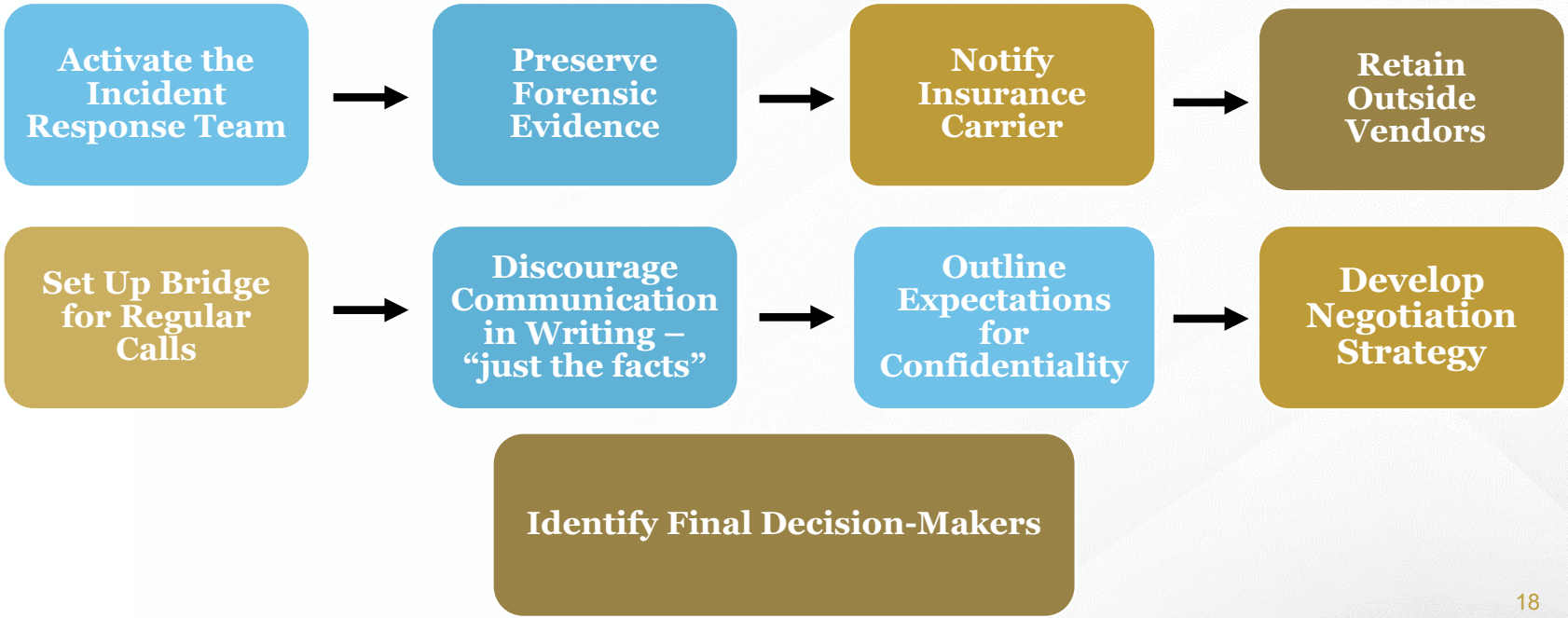
GT GreenbergTraurig

Business Email Compromise

- How it Works:
  - Account takeover (phishing, usually)
  - Identification of impending payment
  - Emails from legitimate account or spoofed address (kevin.scott@gtlaw.com vs. kevin.scott@gtIaw.com)
  - New payment information substituted
  - Immediate transfer of funds
  - B2B lawsuits over who bears the loss

GT GreenbergTraurig

Responding to a Breach: Investigation and Remediation



GT GreenbergTraurig

Responding to a Breach: Notification

Evaluate Whether Notification is Required

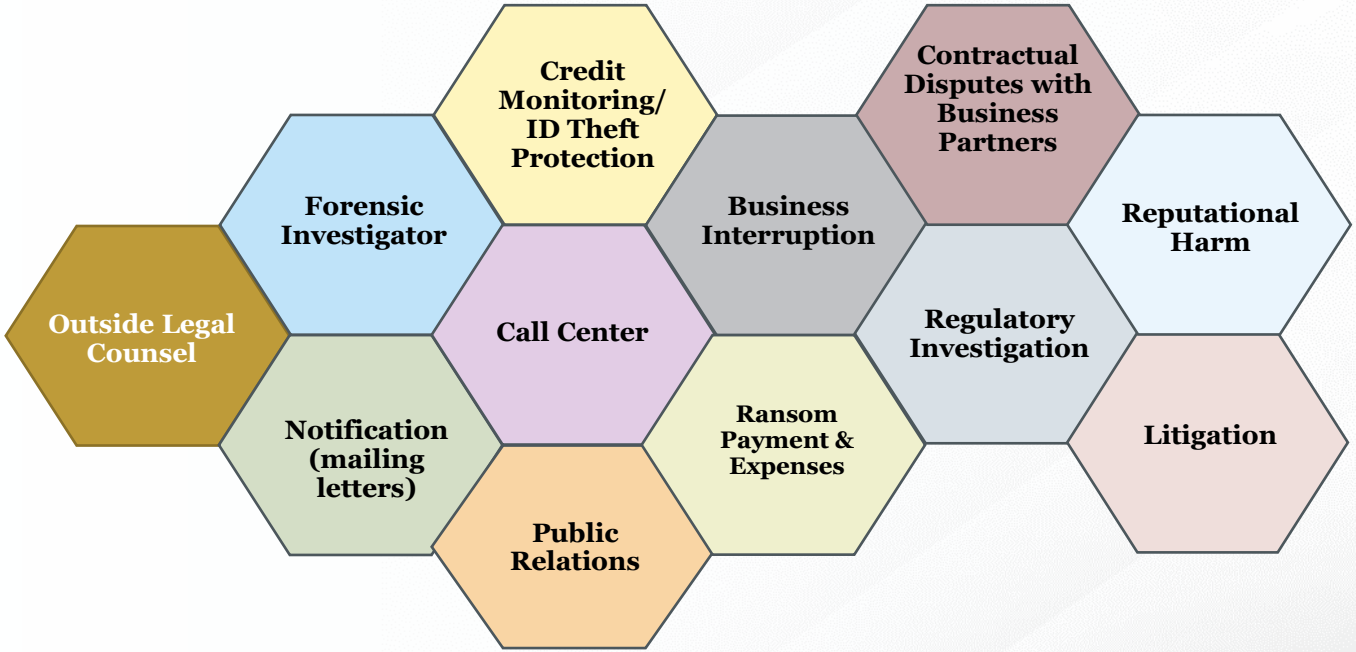
- Identity (credit monitoring and identity theft protection) services
- Call Center
- Website

Develop a Communication Strategy

- Proactive vs. Reactive
- Employee Talking points
- Media Strategy
- B2B Considerations
- B2C Considerations
- Social Media

GT GreenbergTraurig

Costs Associated with a Breach



GT GreenbergTraurig

Evaluate Cyber Insurance Policies

- Companies are increasingly purchasing cyber liability insurance
- Evaluate policies to ensure appropriate coverage, limits, self-insured retention
- Vendor approval
- Extortion coverage: payment, wallet/negotiation assistance
- Bricking
- Reputational Harm
- Exclusions - OFAC

Where are we today?

- ***Loss rates > original estimates***
- ***Premiums*** ↑
- ***Underwriting capacity*** ↓
- ***Underwriting diligence standards hardening = barrier against attackers*** ↑

GT GreenbergTraurig

Cyber Insurance

- **First Party Costs:**
  - Legal counsel
  - Forensic investigator
  - Ransom negotiator/costs
  - Crisis comms (PR)
  - Document review
  - Notification to individuals, regulators
  - Credit monitoring
- **Third Party Costs:**
  - Litigation
  - Regulatory investigations
  - Third party claims
- Ransom payment
- Business interruption loss/extra expense
- Reputational damage
- Also…privacy violations!

GT GreenbergTraurig

Preparing for a Breach

1. Practice the incident response plan – create "muscle memory" – if you can
2. Identify vendors in advance
   - Saves time
   - Pre-negotiate agreement language/rates
3. Know what data you have, where you have it, who has access to it
4. Get rid of data you don't need/use/want

GT GreenbergTraurig

Preparing for a Breach

5. Consider buying cyber insurance
6. Identify an incident response team
7. Develop an incident response plan
8. Identify vendors to assist
9. Gather notification requirements ahead of time
10. Ensure business continuity processes

GT GreenbergTraurig

Preparing for a Breach

11. Evaluate your appetite for paying ransom
12. Test your incident response plan
13. Conduct a Cybersecurity Risk Assessment
14. Can retain third party to identify and address security vulnerabilities
15. Consider all risks, from technical to administrative, to physical
16. Don’t forget about your service providers

GT GreenbergTraurig

Incident Response Plans

- Escalation plan for reporting event/incident
- Identify breach response team – key stakeholders, project manager, decision-makers
- Incorporates legal counsel/privilege
- Identifies applicable regulator/supervisory authorities
- Identifies relevant third parties who may need notification, e.g., business partners, payment processors,
- **Internal/external contact information with back-ups**
- Recordkeeping plan
- Post-incident debrief meeting
- Practice makes perfect (test your plan via tabletop exercises)

GT GreenbergTraurig

U.S. Law Regarding Data Breaches

- All 50 states have their own, similar breach notification laws.
- These laws apply if the *individual* is a resident of that state.
- Certain industries are regulated by federal law (finance, healthcare).
- Only apply if certain personal data elements are exposed –
  e.g., social security number, driver's license number, financial account number, username/password for online account, and sometimes medical/health, insurance, passport number, and biometrics.
- Generally, can conduct a risk assessment.

GT GreenbergTraurig

European Union: GDPR

- Supervisory Authority Notification – within 72 hours of becoming aware of the breach if it's likely there will be a risk to people's rights and freedoms (can do preliminary notice and subsequent reports as breach investigation unfolds).
- Individuals – If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must inform those individuals without undue delay.
- If you do not report, you should document the breach and identify why you didn't report it – justify the decision.

GT GreenbergTraurig

California Consumer Privacy Act (CCPA): A Litigation Game Changer

- First state to provide for statutory damages from a breach.
- $100 - $750 per incident – no need to prove actual damages (but you can)
- Consumer's nonencrypted or nonredacted personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of a business's failure to maintain reasonable security procedures.

GT GreenbergTraurig

Thank You!

Scott Tenenbaum

Head,
North American Cyberclaims
Axis Capital
New York, NY
T: 555.555.1234
Scott.Tenenbaum@axiscapital.com

Kevin M. Scott

Shareholder,
U.S. Data, Privacy & Cybersecurity
Practice, Greenberg Traurig
Chicago, IL
T: 312.456.1040
Kevin.Scott@gtlaw.com

Billy M. Evans, Jr.

Chief Operating Officer,
Kivu Consulting
San Antonio, TX
T: 210.426.8954
nevans@kivuconsulting.com