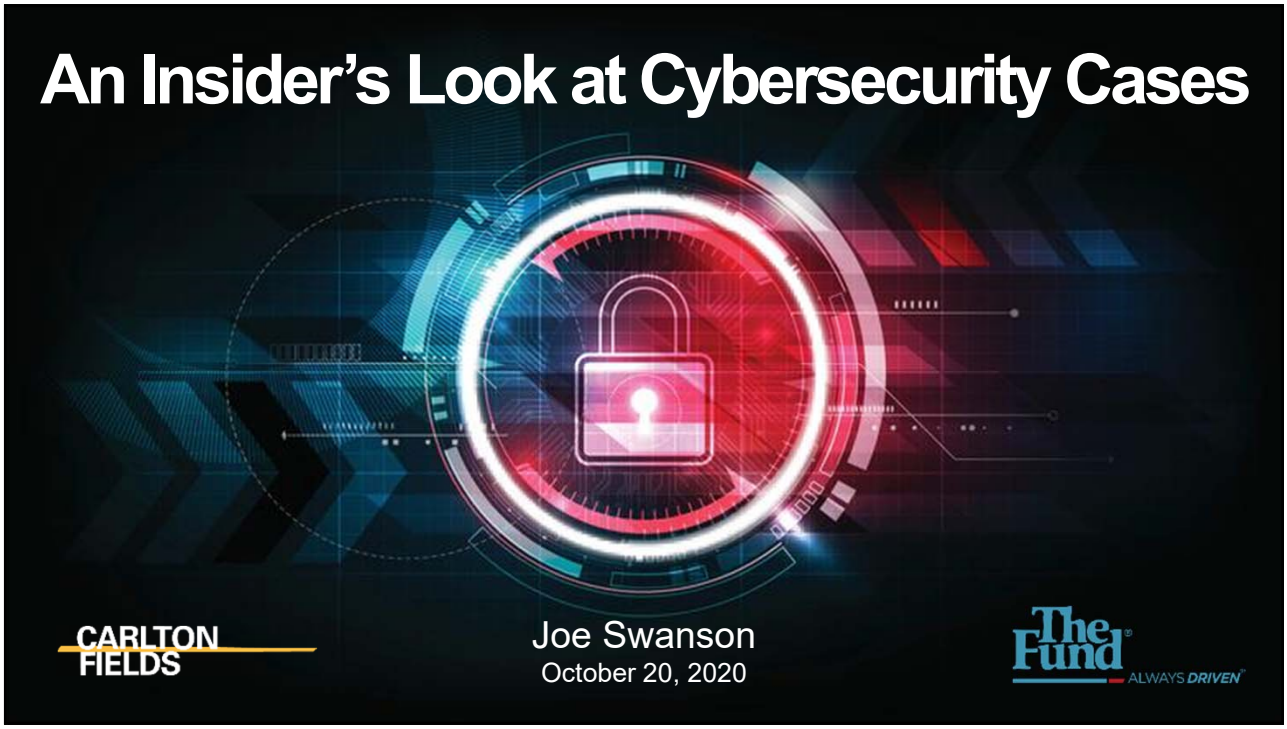
An Insider's Look at Cybersecurity Cases



CARLTON FIELDS

Joe Swanson

October 20, 2020

The Fund ALWAYS DRIVEN

1

Agenda

1. Latest Threats and Case Studies
2. Costs of a Data Breach and Security Incident
3. Best Practices for Preparation and Response
4. Practical Tips

CARLTON FIELDS

The Fund ALWAYS DRIVEN

2

2

1

Latest Threats and Case Studies

CARLTON FIELDS

The Fund ALWAYS DRIVEN

3

3



4

Ransomware: *The Latest Scourge*

- What is it?
  - Malware that locks files and systems
  - May involve data exfiltration, too
- What are the different types?
  - Ryuk, CryptoLocker, Maze
- Massive increase in attacks
  - COVID-19 boom
- Risk of Treasury enforcement
  - Sanctions violations
  - SAR filing obligation

CARLTON FIELDS

The Fund ALWAYS DRIVEN

5

5

Ransomware Incident Response: *Order of Operations*

Phase 1	**Intake**: Learn of the incident
Phase 2	**Internal team**: Assemble incident response team
Phase 3	**External team**: Insurance reporting, then hire as needed, in this order: counsel, forensics, threat actor engagement, rebuild team, media relations.
Phase 4	**Systems work**: Threat actor engagement Assess backups Clean and harden
Phase 5	**Pay or don't pay**
Phase 6	**PII review**: Assess personal information and notice.
Phase 7	**Post-mortem**

CARLTON FIELDS

The Fund ALWAYS DRIVEN

6

6

Ransomware Incident Response

Technical response
- ✓Known variant, with key
- ✓Known bad guy, with track record
- ✓Availability of cryptocurrency

Insurance
- ✓Access to experts, quickly
- ✓Preserving coverage

Failover/failback
- ✓Are the backups clean?
- ✓How much is on there?
- ✓How long will it take?



CARLTON FIELDS

The Fund ALWAYS DRIVEN

7

7

Business Email Compromise: *A Growing Epidemic*

- Scam involving compromised or "spoofed" email accounts
  - Use of social engineering and/or computer intrusion
  - Targeting wire transfers
  - Foreign bank accounts – China, Hong Kong, UK, Mexico, Turkey
    - Domestic money mules
- In 2019, FBI's IC3 received 23,775 BEC complaints
  - Losses of over $1.7 billion
  - That is more than double the losses from 2017
- Growing sophistication
  - Fraudulent verification
  - Artificial intelligence/machine learning – spoofed voices

CARLTON FIELDS

The Fund ALWAYS DRIVEN

8

8

Business Email Compromise: *What To Do*

- Controls
  - Two-factor authentication to prevent unauthorized access
  - Confirm payments without relying on information in the email (consider code phrases)
- Training for Employees
- Develop Law Enforcement Relationships
  - FBI (IC3, Recovery Asset Team) Secret Service (EC
  - FinCEN Rapid Response Program

CARLTON FIELDS

The Fund ALWAYS DRIVEN

9

9

Business Email Compromise: *Who pays?*

- Unsettled law with a variety of legal theories:
  - Negligence
  - Breach of Contract (written or implied)
  - Breach of Fiduciary Duty
  - Violation of Consumer Protection Act
- Most claims settle without a determination of liability
- Best practices
  - Assume a duty exists
  - Educate, train, and communicate
  - Show your work
  - Watch what you say (i.e., don't over-promise)

CARLTON FIELDS

The Fund ALWAYS DRIVEN

10

10

Business Email Compromise: *Role of Insurance*

- Which policy responds?
  - Cyber policy
  - E&O policy
  - Crime policy
- Did the scheme involve a computer? Was there hacking?
- Any intervening events (e.g., a phone call)?
- Who is covered?
  - Employees
  - Clients
  - Sellers
  - Others

CARLTON FIELDS

The Fund ALWAYS DRIVEN

11

11

COVID-19: *Work From Home Risks*

- Rapid incorporation of new technologies
- New methods and types of data being collected and transferred
- Increased reliance on technology, increases hackers' opportunity and leverage
- Distracted employees
- Weaknesses in employees' home networks and computers
- Increasing number of attacks
  - Phishing
  - Business email compromise
  - Malware, including ransomware
- Company files getting lost in the mail

CARLTON FIELDS

The Fund ALWAYS DRIVEN

12

12

2

Costs of a Data Breach and Security Incident

CARLTON FIELDS

The Fund ALWAYS DRIVEN

13

13

2019 Data Breach Trends (>1m records)



- Malicious attacks (most expensive) increased and caused 51% of breaches
- Insiders were responsible for 31% of data breaches
- Nation-state or state-affiliated actors were involved in 23% of breaches
- Timing:
  - 56% of breaches took months or years to discover
  - Average time from data breach incident to containment increased 4.9% to 279 days

IBM Security, Ponemon Institute, *Cost of a Data Breach Report 2019*, available at https://www.ibm.com/security/data-breach; Verizon, *2019 Data Breach Investigations Report*, available at https://enterprise.verizon.com/resources/reports/dbir/.

CARLTON FIELDS

The Fund ALWAYS DRIVEN

14

14

Breach Costs (>1m records)



- Average cost for U.S. data breach: $3.54 million (increased 130% in last 14 years)
- About 1/3 of data breach costs occurred more than a year after the breach
  - Year 1: 67%
  - Year 2: 22%
  - Year 3+: 11%
- Greatest cost of a data breach: Lost business (average: $1.42 million)
- Having an incident response team and extensive response plan testing: $1.23 million savings

IBM Security, Ponemon Institute, *Cost of a Data Breach Report 2019*, available at https://www.ibm.com/security/data-breach.

CARLTON FIELDS

The Fund ALWAYS DRIVEN

15

15

3

Best Practices for Preparation and Response

CARLTON FIELDS

The Fund ALWAYS DRIVEN

16

16

Make an Initial Assessment

1

- **Intake** of the potential **security event**
- Determine the nature of the event:
  - Vulnerability?
  - Breach with access?
  - Breach with acquisition?
  - System unavailability?
  - Impact critical infrastructure operations?
- Determine the **type of information** that may have been exposed
- Locate the **incident response guide** and begin the process

CARLTON FIELDS

The Fund ALWAYS DRIVEN

17

17

Assemble the Incident Response Team (Internal)

2

Legal	Executive	CISO	Media Relations
HR	Business Unit	Risk Manager	IT Lead
	Customer Relations		

CARLTON FIELDS

The Fund ALWAYS DRIVEN

18

18

Who Helps the Incident Response Team (External)?

2

- Early on:
  - Insurance broker
  - Insurance carrier
  - Counsel
  - Forensics experts
  - Breach coach
- A little later:
  - Law enforcement
  - Public relations pros
  - Credit monitoring
  - Call centers / mailing houses

CARLTON FIELDS

The Fund ALWAYS DRIVEN

19

19

Start Investigation and Mitigation

3

- Reassess the initial assessment with the full team
- Determine if the breach is active
- Identify all affected systems, computers, and devices
- Identify the data, if any, at issue
- Interview key personnel
- Determine the cause of the breach
- Deploy technical mitigation efforts
- Determine when systems can be brought back online
- Use alternative communication channels as needed

CARLTON FIELDS

The Fund ALWAYS DRIVEN

20

20

Preserve Records of the Breach and Mitigation



- Preserve evidence of the breach, including log files
- Control the creation of new documents and records
- Document all efforts to investigate and mitigate the breach
- Involve the legal department and outside counsel as necessary, which may help to preserve the attorney-client and work product privileges

CARLTON FIELDS

The Fund ALWAYS DRIVEN

21

21

Determine Legal Notification Obligations



- Law enforcement
- State attorneys general
- Impacted customers or employees
- Acquiring bank and card brands (for credit card breaches)
- Regulators
- Credit reporting agencies
- Contract partners (if required by contract)

CARLTON FIELDS

The Fund ALWAYS DRIVEN

22

22

The Typical Data Security Statute (Florida)



- "Each covered entity … shall take **reasonable measures** to protect and secure data in electronic form containing personal information."
- "'Breach [ ]' means **unauthorized access** of data in electronic form containing **personal information** … ."
- No focus on privacy, just data security and notice.

- If there is a breach, a company must provide **notice**:
  - "to each individual **in this state** whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach."
  - "as expeditiously as practicable and without unreasonable delay . . . but no later than **30 days** after the determination of a breach or reason to believe a breach occurred."
  - to the Attorney General if **500 or more** Floridians.

CARLTON FIELDS

The Fund ALWAYS DRIVEN

23

23

Gramm-Leach-Bliley Act



- GLBA imposes significant requirements on financial institutions related to privacy and security of customer data
  - Privacy notice and opt-out of information sharing
  - Assess and implement controls for risks to customer data
  - Employee training and management
  - Information systems
  - Detection, prevention, and response to cyber attacks and system failures
    - Includes breach notification obligations (regulator, SAR, customers)

CARLTON FIELDS

The Fund ALWAYS DRIVEN

24

24

Interacting with Law Enforcement

4



CARLTON FIELDS

The Fund ALWAYS DRIVEN

25

25

Should You Reach Out to Law Enforcement During an Incident?

4

Make this question part of your incident response plan

If NOT required, consider factors against outreach:

- Possible liability
- Disruption of business
- Possibility of increased publicity
- Confidentiality concerns

Compelling reasons in favor of outreach:

- LE might be notified anyway
- Benefit from LE's tools and relationships
- Manage the situation
- Mitigate liability
- Delayed public notification
- Deterrent effect

CARLTON FIELDS

The Fund ALWAYS DRIVEN

26

26

Tips for Working with Law Enforcement

4

- **Identify a single point of contact for law enforcement**
  - Speeds communication with LE
  - Task with "chain of custody" and big picture
- **Interview IT and other knowledgeable staff**
  - Identify witnesses
  - Identify sources of evidence
- **Preserve the evidence**
  - IP logs, system access, suspicious calls/emails
  - Cease routine overriding of data
- **Draft a "prosecution memo"**
  - Lays out the crimes, evidence, and other factors
  - Agents will use it as a roadmap when talking to prosecutor



CARLTON FIELDS

The Fund ALWAYS DRIVEN

27

27

Contract Counterparties: *When Your Best CUSTOMER….*

4

1. Causes you to be breached

Very hard to sue them
Often you can extract a discount
Reform the contract to better spread the risk

2. Is the victim of your breach

Tell them even if not required by law or contract
Provide discounts
Allow audits or input on controls

CARLTON FIELDS

The Fund ALWAYS DRIVEN

28

28

Post-mortem Assessment



- Determine the root cause of the data breach
- Revise the incident response guide
- Evaluate the performance of the incident response team
- Assess deployment of information security resources

CARLTON FIELDS

The Fund ALWAYS DRIVEN

29

29

4

Practical Tips

CARLTON FIELDS

The Fund ALWAYS DRIVEN

30

30

Security Strategies

- Privileged access management
- Security settings
- Threat identification and response
- Data protection and encryption
- Social engineering awareness

CARLTON FIELDS

The Fund ALWAYS DRIVEN

31

31





Joe Swanson
Carlton Fields

Phone: 813.229.4335
jswanson@carltonfields.com

CARLTON FIELDS

The Fund ALWAYS DRIVEN

32

32