Data Privacy & Cybersecurity: What Boards Needs to Know

PCCE Directors' Academy

September 21, 2023

Lesson #1
Know Your Company and Risk Profile

Consider

- How big is your business?
- Where does your company operate?
- Where are your employees or contractors located? Are any remote? (And are any in North Korea?)
- What kinds of data and assets do you have?
- What kinds of third parties do you rely on?
- Who are your customers?
- What's the maturity level of your cybersecurity and privacy compliance programs?

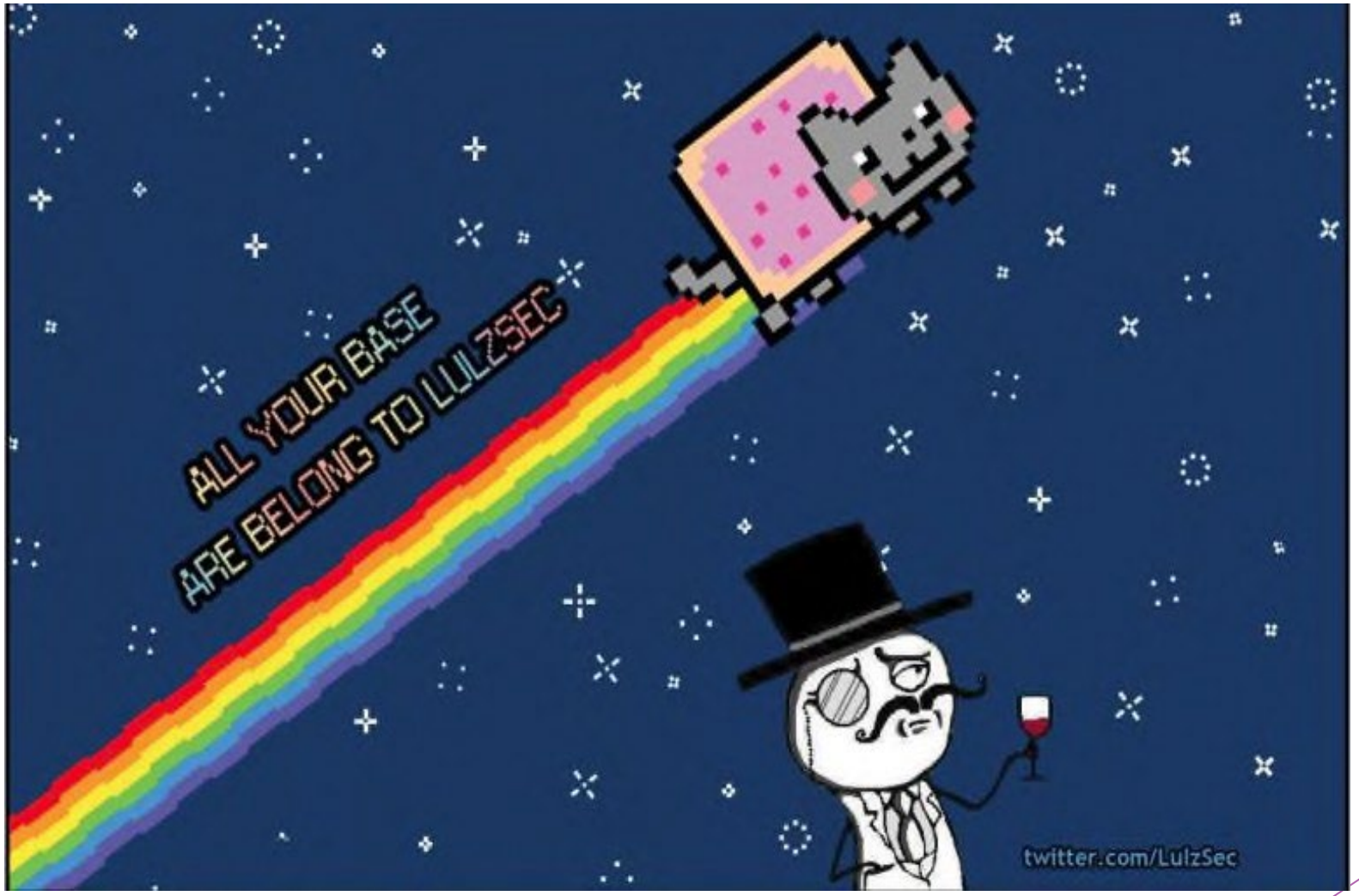
Why it Matters

- What assets/data/systems are threat actors most likely to target?
- What are your vulnerabilities?
- Is your cybersecurity program receiving enough funding and support?
- What laws and regulatory regimes apply to your company?

Equifax managed "almost 1,200 times" the amount of data held by the Library of Congress, much of it sensitive, yet its cybersecurity program was rated 0 out of 10 in the years before it was breached

Lesson #2
Know Who the Threat Actors Are and What They Want

Who are the bad actors?



Who are they and what do they want?

- **State Sponsored**

  Espionage, Trade Secrets, Money, Acts of War/Destruction, Destabilization, Misinformation

  China, Russia, Iran, North Korea and …

  … the United States

- **"For Profit"**

  Money (bank robbers, con artists, and extortionists with computers)

- **"Hacktivists"**

  Political Agendas, Disruption, Intimidation, Fame, "Lulz"

- **Insiders**

  Any/all of the above

Why it Matters

- What kind of threat actors are likely to target you and why?
- How sophisticated are they likely to be?

SolarWinds provided essential IT services to large corporations and government agencies – making it a target (and a vector) for a very sophisticated supply chain attack by alleged Russian state actors.

Lesson #3
Most Successful Attacks Rely on Either Human Error or the Exploitation of Trust

Human Error

THE WALL STREET JOURNAL.

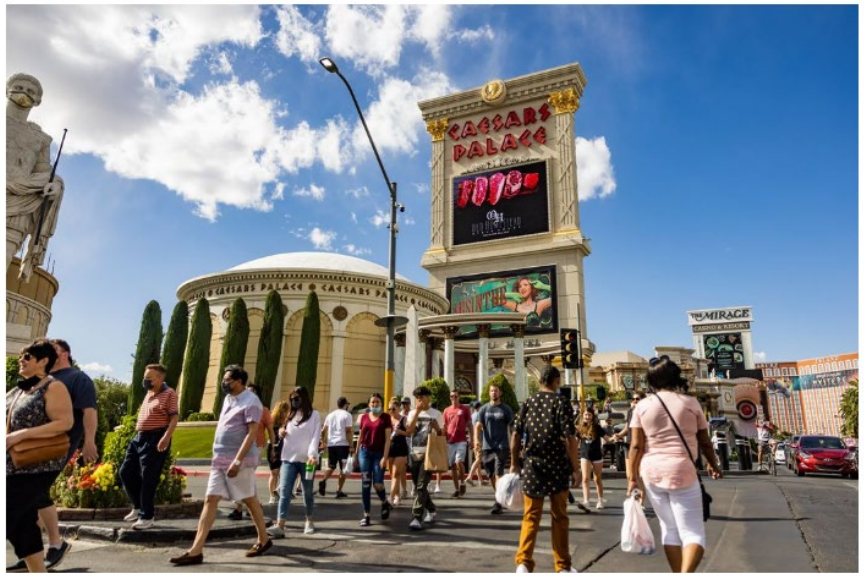
Caesars Paid Ransom After Suffering Cyberattack

Caesars is second major casino operator hit by hackers in recent weeks

By Katherine Sayre Follow and Robert McMillan Follow

Updated Sept. 14, 2023 10:03 am ET

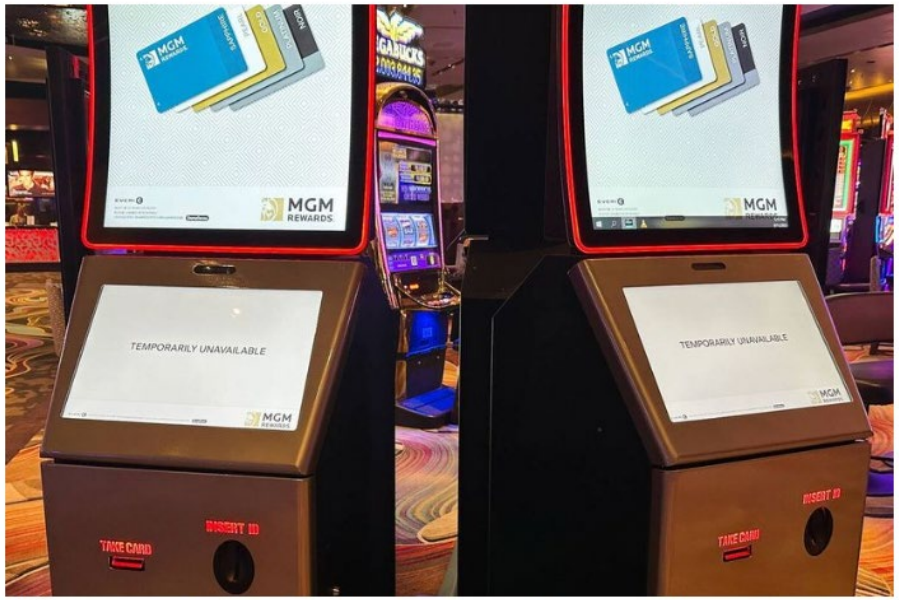
Gift unlocked article | Listen (7 min)



Caesars Entertainment, which operates Caesars Palace in Las Vegas, is expected to report the cyberattack in an SEC filing. PHOTO: ROGER KISBY/BLOOMBERG NEWS

Pro Take: MGM Casino Hack Shows Challenge in Defending Connected Tech

The attack shows how hacks can significantly disrupt operations



Kiosks were out of service at MGM's Aria Resort and Casino in Las Vegas on Monday.

PHOTO: DANIEL PEARSON/LAS VEGAS REVIEW-JOURNAL/TNS/GETTY IMAGES

By James Rundle

Sept. 14, 2023 5:30 am ET | WSJ PRO

Human Error

Caesars

- *Social-engineering attack on a third party vendor*

MGM

- *Social-engineering attack on MGM to force password reset*

Human Error: Equifax

- Error #1 – Internal scans missed an instance of vulnerable code within Equifax
- Error #2 – Patch management policy was outdated
- Error #3 – Storage of access credentials in the clear
- Error #4 – Expired SSL certificate prevented Equifax from monitoring network traffic
- Error #5 – Default setting allowed web traffic to pass even when monitoring device certificate was expired

Exploitation of Trust

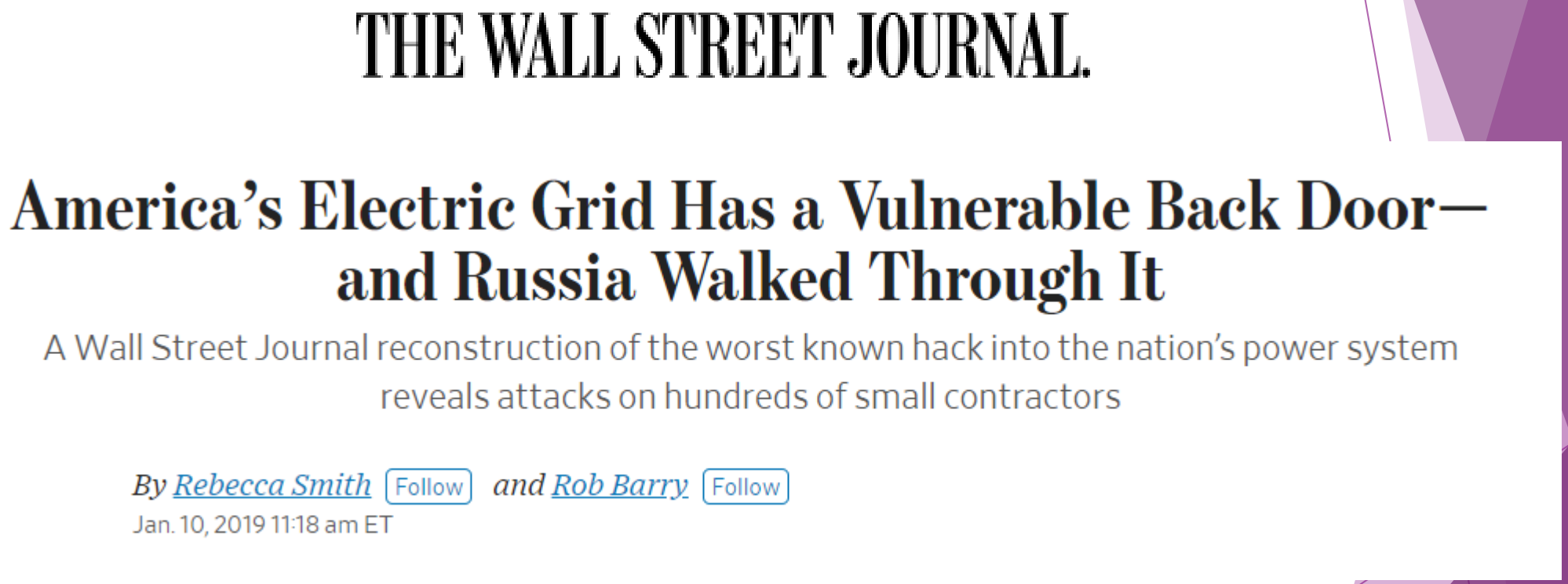
SolarWinds

- *Threat actors gain access via software from trusted third party*

Target

- *Threat actors gain access via network connection from trusted third party*

Exploitation of Trust



THE WALL STREET JOURNAL.

America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors

By Rebecca Smith Follow and Rob Barry Follow

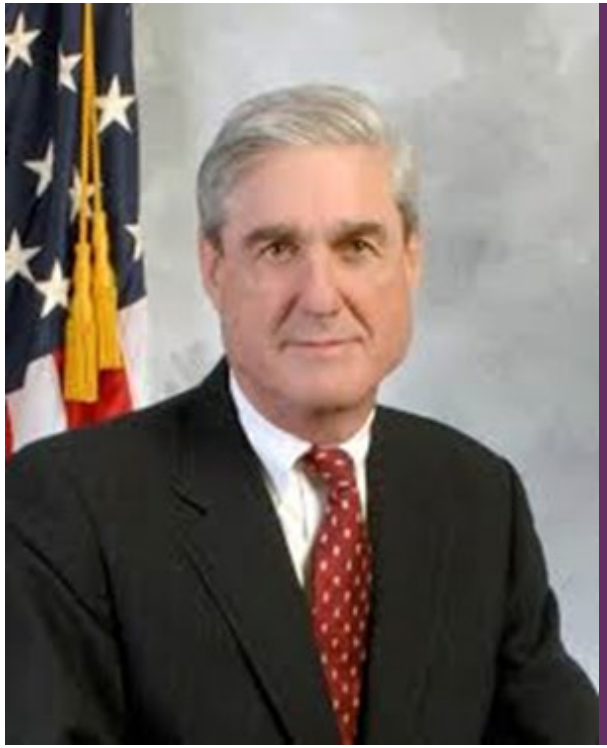
Jan. 10, 2019 11:18 am ET

Why it Matters

In the end, most hackers will gain access to your systems and data because you, your employees, or your third parties let them in

Lesson #4
A Cyber or Privacy Incident Is Inevitable and You Must Be Ready to Respond

Cyber & Privacy Incidents Are Inescapable



I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.

– Former FBI Director Robert S. Mueller III (March 2012)

Why it Matters

- How you respond to an incident can determine how much legal, reputational, and economic risk you face in the aftermath
- Incident response plans are mandatory under some laws
- The first time management and the board think about how to respond to an incident shouldn't be when an incident is happening
- Have vendors ready to go – and have a plan for legal privilege
- Some laws – like the SEC's new disclosure regs, GDPR, NYDFS regs – greatly reduce the amount of time firms have to figure out what is happening and to make a decision on whether the breach should be reported
- Do you know how to call the FBI and actually have someone pick up the phone?

Responding Quickly

Caesars

- Social-engineering attack on a third party vendor
- After identifying the attack, promptly activated incident response plan, got outside help, notified law enforcement
- Attackers got access to loyalty program database; SSNs and Driver's License #s
- Reportedly paid half of $30M demand from hackers; took steps to get threat actors to delete data
- Filed 8-K, will notify customers

MGM

- Social-engineering attack on MGM to force password reset
- After identifying the attack, promptly activated incident response plan, shut down some systems; got outside help, notified law enforcement
- Unclear if hackers got access to any data; filed 8-K
- Reportedly has not paid any ransom; took several days for all systems to recover
- Estimates lost $4m - $8m/day

Lesson #5

The Board's and the Company's Legal Obligations and Risk Are Increasing

SolarWinds

- IT infrastructure company
- Orion product monitors and manages network systems
- Hackers breached SolarWinds – potentially through weak passwords – and inserted malware into the Orion product
- Between March and June 2020, SolarWinds distributed corrupted updates of Orion to up to 18,000 of its customers
- Hackers used the malware embedded in Orion to steal data from as many as 100 of SolarWinds' private sector and government customers
- In December 2020, SolarWinds detects the issue, notifies customers, and releases patches for Orion

SolarWinds *Caremark* Litigation

- Plaintiffs Alleged:
  - Board delegated cyber oversight to committees
  - Committees received reports that detailed lapses in cybersecurity program prior to incident
  - No full board briefing on cybersecurity for two years prior to the incident
  - Evidence of weak password controls in the years prior to incident
- Dismissed for failure to adequately plead demand futility:
  - Directors did not cause a violation of "positive law"
  - Directors ensured the company had a minimal cyber reporting system
  - No allegations directors ignored "red flags" of cyber threats to imply bad faith

Case Study: SolarWinds *Caremark* Litigation

- Cybersecurity for SolarWinds was "mission critical" but is also a "business risk" that, absent bad faith, is an exercise of business judgment
- Delegation of cyber risk to a "non-sham, functioning committee" was OK even if reporting to the full Board was "subpar" as long as there was not an "utter failure to attempt to assure" that a reporting system existed
- Even though cybersecurity is important, *Caremark* claims don't typically survive unless the Board was involved in causing the firm to violate a "positive law"

“Positive Laws”

- Federal, State & Int’l Criminal Laws
- Federal Statutes
  - Federal Trade Commission Act
  - Gramm-Leach-Bliley Act
  - Fair Credit Reporting Act
  - HIPAA
  - COPPA
- Federal Regulations
  - FTC Health Data Breach Rule
  - SEC Cyber Disclosure Rule, etc.
- SRO Rules (FINRA, NFA, etc.)
- State Laws
  - “Mini” FTC acts
  - Breach notification laws
  - NYDFS Cybersecurity regulations
  - State privacy laws (13 and counting)
  - Cybersecurity laws (e.g., NY Shield Act)
- Foreign Laws
  - GDPR
  - Other foreign data protection and breach notification laws

“Positive Laws”

- NY Shield Act – *requires reasonable safeguards to protect personal data*
- State privacy laws (e.g., CCPA) - *requires reasonable safeguards to protect personal data*
- NYDFS Cybersecurity Rules – *requires comprehensive cybersecurity program; regular board reporting; and board-approved cyber policies*
- FTC Act – *requires reasonable cybersecurity program*

New SEC Cyber Disclosure Rules

- Must disclose within four business days of determining that a cybersecurity is material
- Materiality determination must be made without unreasonable delay
- A series of non-material incidents could be material in the aggregate
- Need not disclose specific or technical information about response
- Duty to provide updates and amendments as new information becomes available
- May be delayed for national security or public safety reasons if approved by the U.S. Attorney General

New SEC Cyber Disclosure Rules

- Requires detailed disclosure regarding issuers' cyber risk assessment programs, including assessment of third party risk
- Disclosure of material cyber risks
- Disclosure of the board's oversight of and management's role in assessing and managing cyber risks
- Must disclose cyber expertise of senior management (but not board expertise)

Why it Matters

- Cybersecurity and privacy laws expose firms to increased litigation and regulatory risk
- Regulators like the SEC and FTC looking to make examples of firms for obvious missteps or lapses
- Some laws have private rights of action with statutory damages
- An actual violation of law might improve a plaintiff's chances in a *Caremark* case

Lesson #6
Don’t Forget the Privacy Revolution

What's Going On?

- 13 states have passed GDPR-like consumer privacy laws (California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Montana, Florida, Texas, Oregon, and Delaware)
- No two are same
- All create new data rights for consumers
- All require privacy programs and privacy risk assessments
- Some place limits on data processing activities; profiling, "dark patterns"; use of sensitive data, etc.
- Laws differ in application to employee data, health data, non-profits, etc.

What's Going On?

- FTC has been aggressive in pursuing enforcement actions for privacy violations; seeking to promulgate potential new regulations
- Laws with private rights of action (e.g., Illinois's Biometric Information Privacy Act (BIPA)) continue to be a boon to the plaintiffs' bar

Why it Matters

- New laws may curtail or restrict the way firms use personal data
- Laws will require firms to place more controls around personal data processing and conduct risk assessments and increase oversight responsibilities for boards
- Firms' business teams should be considering the privacy implications of new products, services, and apps from inception, during development, and throughout the product lifecycle
- Regulators are looking to make examples of firms that mishandle or exploit personal information