

Hackers Will Find a Way: Cybersecurity Preparedness and Incident Response in Post-Jurassic Times

Evan Foster

Steven Blickensderfer

Alexander (Sandy) Bilus

Kenneth Oh

September 12, 2024

Topics for Today's Discussion



Cybersecurity Threat Landscape



Preparing for a Cybersecurity Attack



Responding to a Cybersecurity Attack

THE CYBERSECURITY THREAT LANDSCAPE



The Cybersecurity Threat Landscape

SolarWinds' Ruling 'No Comfort' For Cybersecurity Leaders

By Jessica Corso · Listen to article

Law360 (July 19, 2024, 9:07 PM EDT) -- Although a federal district court has struck down significant portions of the U.S. Securities and Exchange Commission's data breach case against software developer SolarWinds Corp., attorneys say what remains of the lawsuit gives "no comfort" to chief information security officers hoping to avoid similar suits over statements about their company's cybersecurity practices.

U.S. District Judge Paul Engelmayer on Thursday threw out the majority of the claims that the SEC brought against SolarWinds after the company was hit with a Russia-linked cyberattack that compromised the networks of many of its clients, including several federal agencies.

The company said in a statement following the ruling that it was pleased that the judge largely granted its motion to dismiss, but it will still have to fend off allegations that it and its chief information security officer, Timothy Brown, committed securities fraud by publicly declaring SolarWinds' cybersecurity practices to be more robust than they actually were.

"The outcome at this stage should give CISOs no comfort about their need to be very careful about how things they say and do could be misinterpreted and they could be held personally accountable," Reed Smith LLP partner Gerard M. Stegmaler told Law360 on Friday.

Brown became the first corporate executive sued by the SEC in a cybersecurity breach case when the agency named him a defendant in the SolarWinds suit last year.

His inclusion in the case has faced controversy and left other CISOs and cybersecurity professionals worried that their role in safeguarding IT infrastructure could be compromised by fears that internally flagging potential safety issues could lead to an SEC enforcement action.

"Often the CISOs are the truth-tellers inside their organizations, they are the canaries sometimes in coal mines," said Stegmaler, who counsels clients on data protection issues. "If you're going to kill the canary for chirping, that's a really bad move if your goal and endeavor is to ensure safety in the coal mine."

The SEC said an internal presentation given by Brown demonstrated that he knew about the company's cybersecurity vulnerabilities years before the 2020 hack but still signed off on a statement posted to SolarWinds' website touting the company's strong cybersecurity practices.

Useful Tools & Links

- Add to Briefcase
- 📄 Save to PDF & Print
- 🗨️ Flag/Report
- 👤 Editorial Contacts

Related Sections

- 📄 Aerospace & Defense
- 📄 Capital Markets
- 📄 Compliance
- 📄 Corporate
- 📄 Cybersecurity & Privacy
- 📄 Government Contracts
- 📄 Securities
- 📄 Technology

Case Information

CHRISTOPHER BRUCKMANN
(SDNY Bar No. CB-7317)
Attorney for Plaintiff
SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, D.C. 20549
(202) 551-5986
BruckmannC@sec.gov

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,)
Plaintiff,)
v.)
SOLARWINDS CORP. and TIMOTHY G.)
BROWN,)
Defendants.)

Civil Action No. 23-cv-9518

Jury Trial Demanded

COMPLAINT

Plaintiff Securities and Exchange Commission ("SEC"), for its Complaint against Timothy G. Brown

July 26, 2024, 12:17 PM EDT

Rite Aid Sued Over Data Breach Said to Affect 2.2 Million People


Christopher Brown
Staff Correspondent

- COURT: E.D. Pa.
- TRACK DOCKET: No. 2:24-cv-03356

Rite Aid Corp. failed to protect the personal information of 2.2 million people that was exposed in a June data breach, a proposed federal class action said.

Margaret Bianucci alleged that the national drugstore chain breached its duties under common law and the Federal Trade Commission Act to safeguard sensitive data, and failed to implement reasonable and adequate data security measures or comply with

Cost of a Data Breach Report 2024



Bloomberg Law

In-house legal teams save 200+ hours a year on legal work

Federal Gov't Hits Georgia Tech With Cybersecurity FCA Suit

By Daniel Wilson · Listen to article

Law360 (August 23, 2024, 6:46 PM EDT) -- The federal government has hit the Georgia Institute of Technology with a False Claims Act suit accusing the university of knowingly failing to comply with required cybersecurity standards while working on federal defense contracts.

Georgia Tech's Astrolavos Lab failed to develop a required system security plan and didn't use antivirus tools, the U.S. Dept. of Justice said.

Attached Documents

- Complaint


Kurt the CyberGuy

AP AP News

Data breach at MGM Resorts expected to cost casino giant \$100 million

The data breach that MGM Resorts is calling a cyberattack is expected to cost the casino giant more than \$100 million.

Oct 6, 2023



Data breach victims skyrocket over 1,100%: How to protect yourself



data breach victims in the second quarter of 2024 was 1170% higher than the time last year.

CybersecurityNews

TOYOTA Data Breach - Hackers Group Leaked 240 GB of Data Online

TOYOTA Data Breach, allegedly perpetrated by the notorious hacker group ZeroSevenGroup, has exposed a wide array of data.

2 weeks ago



Threat: Ransomware

- Exploit vulnerability
- Gain access to data
- Exfiltrate data
- Encrypt the system

How does it work?



- Unable to use system
- Exposure of data
- Loss of money
- Reputational harm

How can it harm a business?



Threat: Business Email/Text Compromise

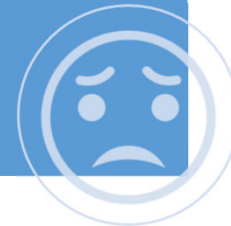
- Exploit vulnerability
- Gain access to data
- Send fraudulent wire transfer instructions

How does it work?



- Loss of money
- Relationship harm
- Exposure of data

How can it harm a business?



PREPARING FOR A CYBERSECURITY ATTACK



Three Key Ways to Prepare

Information
Security
Program

Incident
Response Plan

Training and
Awareness
Building

Incident Response: A Playbook

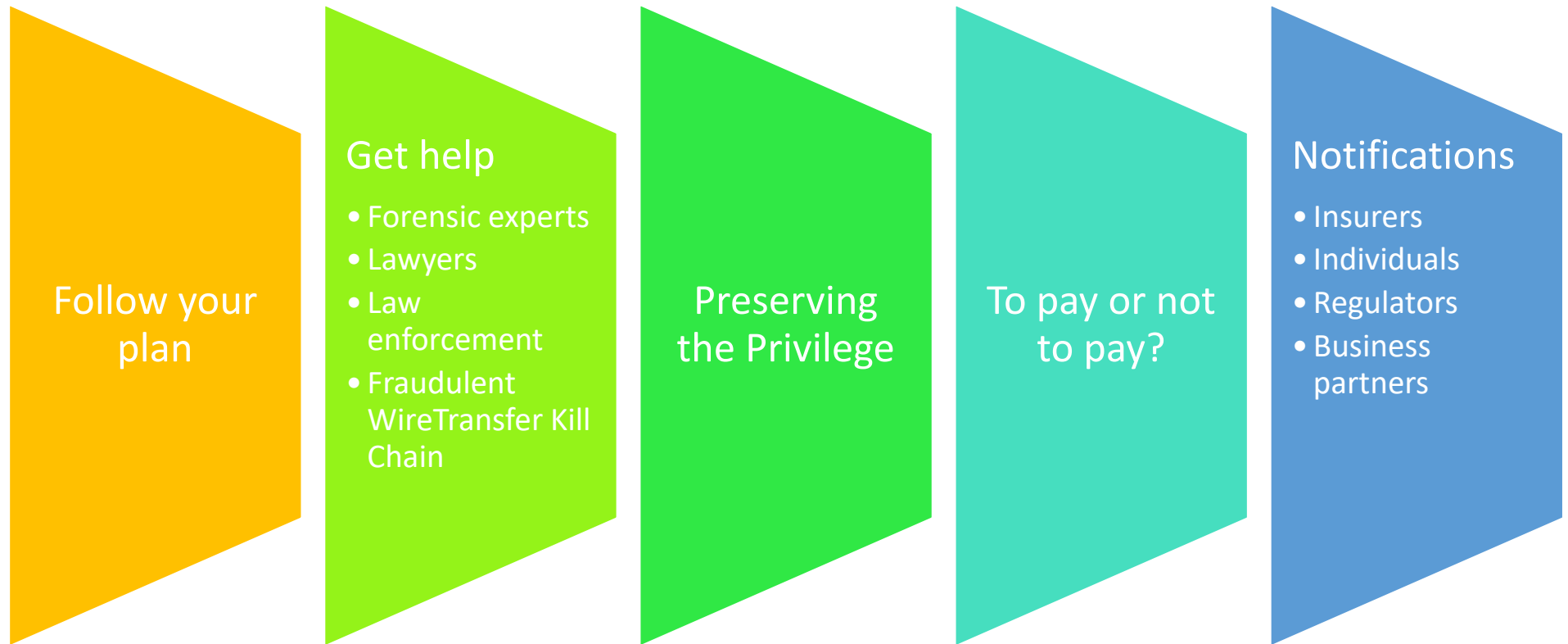
- (1) What constitutes an incident and its severity (downtime, lost sales, etc.)?
- (2) Who makes the determination (before going to the executives)?
- (3) Who are part of the core and extended team?
- (4) How do you send out and track privilege memos (what if system is down)?
- (5) How do you contact people, including board members (if emails are offline)?
- (6) Who needs to know, who contributes, and who are the decisionmakers (especially SEC filings)?
- (7) Who are the key suppliers that must know and how do you contact them?
- (8) How do you engage cybersecurity vendors (identity theft & forensics vendors)?
- (9) How do you contact law enforcement (e.g., contact secret service for kill chain)?
- (10) How do you keep information current?
- (11) How do you communicate data breach to consumers?
- (12) How do you stress test the Playbook (e.g., tabletop exercise)?

RESPONDING TO A CYBERSECURITY ATTACK



SAUL EWING

Issues that Arise During Incident Response



Don't Be A Fossil



A Take Home To-Do List

Written Information Security Program

- Risk assessment
- Administrative, technical, and physical safeguards
- Vendor oversight
- Test effectiveness of the safeguards

Incident Response Plan

- Define roles, responsibilities, and levels of decision-making authority
- Communications methods
- Contact information

Training & Awareness Building

- Hire vendors that can provide training on cybersecurity incidents
- Involve your IT and security staff
- Conduct a tabletop exercise

Baltimore

1001 Fleet Street
9th Floor
Baltimore, MD 21202
T: (410) 332-8600 • F: (410) 332-8862

Boston

131 Dartmouth Street
Suite 501
Boston, MA 02116
T: (617) 723-3300 • F: (617) 723-4151

Chesterbrook

1200 Liberty Ridge Drive
Suite 200
Wayne, PA 19087
T: 610.251.5050 • F: (610) 651-5930

Chicago

161 North Clark Street
Suite 4200
Chicago, IL 60601
T: (312) 876-7100 • F: (312) 876-0288

Fort Lauderdale

200 E. Las Olas Blvd.
Suite 1000
Fort Lauderdale, FL 33301
T: (954) 713-7600 • F: (954) 713-7700

Harrisburg

Penn National Insurance Plaza
2 North Second Street, 7th Floor
Harrisburg, PA 17101
T: (717) 257-7500 • F: (717) 238-4622

Los Angeles

1888 Century Park East
Suite 1500
Los Angeles, CA 90067
T: (310) 255-6100 • F: (310) 255-6200

Miami

701 Brickell Avenue
17th Floor
Miami, FL 33131
T: (305) 428-4500 • F: (305) 374-4744

Minneapolis

33 South Sixth Street
Suite 4750
Minneapolis, MN 55402
T: (612) 225-2800 • F: (612) 677-3844

New York

1270 Avenue of the Americas
Suite 2800
New York, NY 10020
T: (212) 980-7200 • F: (212) 980-7209

Newark

One Riverfront Plaza
1037 Raymond Blvd., Suite 1520
Newark, NJ 07102
T: (973) 286-6700 • F: (973) 286-6800

Orange County

5 Park Plaza
Suite 650
Irvine, CA 92614
T: (949) 252-2777 • F: (949) 252-2776

Philadelphia

Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102
T: (215) 972-7777 • F: (215) 972-7725

Pittsburgh

One PPG Place
Suite 3010
Pittsburgh, PA 15222
T: (412) 209-2500 • F: (412) 209-2570

Princeton

650 College Road East
Suite 4000
Princeton, NJ 08540
T: (609) 452-3100 • F: (609) 452-3122

Washington, D.C.

1919 Pennsylvania Avenue, N.W.
Suite 550
Washington, DC 20006
T: (202) 333-8800 • F: (202) 337-6065

West Palm Beach

515 N. Flagler Drive
Suite 1400
West Palm Beach, FL 33401
T: (561) 833-9800 • F: (561) 655-5551

Wilmington

1201 North Market Street
Suite 2300 • P.O. Box 1266
Wilmington, DE 19899
T: (302) 421-6800 • F: (302) 421-6813