

November 10, 2023

Shifting Norms in Data Security Incident Response

Kirk Nahra

Partner, WilmerHale

Heidi Wachs

Managing Director, Stroz Friedberg, an Aon Company

Shannon Togawa Mercer

Senior Associate, WilmerHale



Kirk Nahra

Partner
WilmerHale
@KirkJNahrawork
kirk.nahra@wilmerhale.com



Heidi Wachs

Managing Director
Stroz Friedberg, an Aon Company
@hlwachs
Heidi.Wachs@strozfriedberg.com



Shannon Togawa Mercer

Senior Associate
WilmerHale
@togawamercer
shannon.mercer@wilmerhale.com

Agenda

Agenda

- I. Burgeoning Themes in Incident Response for Discussion
- II. Recent Representative Incidents in the News
- III. Vendor Breach Scenario
- IV. Key Stumbling Blocks
 - I. Forensic Investigation
 - II. Determining Impact
 - III. Individual Notifications
 - IV. Regulatory Notifications

Burgeoning Themes in Incident Response for Discussion

- **For discussion today:** Third-party attacks (vendor attacks or supply chain attacks) introducing complexity in response activities
 - Increasing scale of breaches
 - Making analysis of impact, including forensic analysis, complex
 - Implicating third-party relationships, including contractual rights
 - Data breach reporting regimes not set up for vendor – customer breach reporting
- **Other areas seeing increased requirements and complexity:**
 - Increased frequency of ransomware and cyber extortion attacks across sectors, geographies
 - Global comprehensive data protection and data breach laws requiring extensive data breach exposure analysis and notice
 - Increased attention from US regulators across sectors, in some cases requiring more and faster reporting, increased post-incident scrutiny

Recent Representative Incidents in the News

Representative Incidents

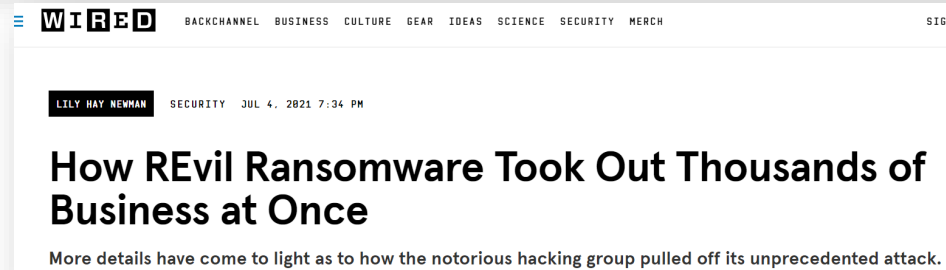
SolarWinds is 'largest' cyberattack ever, Microsoft president says

The hack sent malware to about 18,000 public and private organizations.

The 'most serious' security breach ever is unfolding right now. Here's what you need to know.

Much of the Internet, from Amazon's cloud to connected TVs, is riddled with the log4j vulnerability, and has been for years

By [Tatum Hunter](#) and [Gerrit De Wincq](#)
Updated December 20, 2021 at 5:28 p.m. EST | Published December 20, 2021 at 10:13 a.m. EST



WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY MERCH SIGN

LILY HAY NEWMAN SECURITY JUL 4, 2021 7:34 PM

How REvil Ransomware Took Out Thousands of Business at Once

More details have come to light as to how the notorious hacking group pulled off its unprecedented attack.

Featured Article

MOVEit, the biggest hack of the year, by the numbers

At least 60 million individuals affected, though the true number is far higher

Carly Page @carlypage_ / 11:45 AM EDT • August 25, 2023

 Comment

TECH

Ransomware Attack Affecting Likely Thousands of Targets Drags On

REvil is said to have focused on Kaseya VSA, a software used by large companies and technology-service providers to manage and distribute updates

By [Robert McMillan](#) [Follow](#)
Updated July 4, 2021 12:27 pm ET

Ransomware, Incident Response, Breach

[f](#) [t](#) [e](#) [in](#)

Another 1.3M patients added to data breach tally of ransomware attack on Eye Care Leaders

[Jessica Davis](#) June 16, 2022

Vendor Breach Scenario

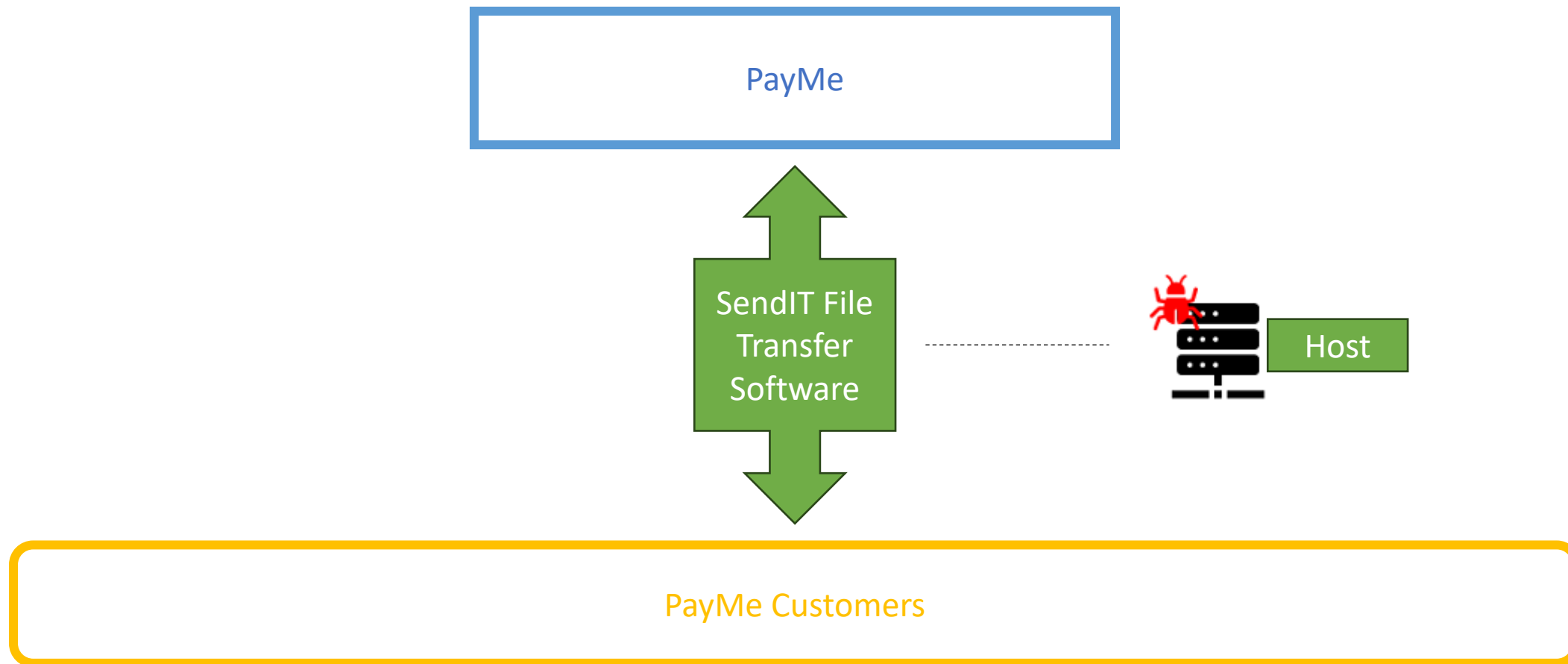
Vendor Breach Scenario

A cyber extortion group exploits a zero day in a file transfer software, SendIT, used by a payroll and healthcare benefits outsourcing company, PayMe Inc., that provides thousands of small and medium sized enterprises in the US, the UK, and the EU with payroll services.

This group claims to have access to millions of PayMe's customers' employee records, including social security numbers in the US, national IDs or other identification, and financial and account information. The group also claims to have health insurance claim information for a subset of employees. Proof of life provided thus far in negotiations confirms that assertion.

To increase pressure on PayMe, the cyber extortion group posts that it has victim data, including PayMe data, on its "name-and-shame" blog on the dark web. PayMe's customers, through their own threat intelligence platforms, learn of the alleged compromise and reach out to PayMe to learn more about the incident.

Vendor Breach Scenario, cont.



Key Stumbling Blocks

If you are a PayMe customer:

- How do you get sufficient and accurate information about your exposure in a timely way? Can you, or do you, rely on the information you're getting?
- If PayMe is in the middle of negotiations with the threat actor, how can you influence those negotiations? Do you hire your own ransomware negotiating team for threat intelligence and advice?

If you are PayMe:

- How are you liaising with SendIT to understand the scope of access?
- How do you provide transparency to customers in the middle of an evolving investigation?
- Is your forensic investigation team getting the information it requires from SendIT to conduct a thorough investigation?

Key Stumbling Blocks: Determining Impact

If you are a PayMe customer:

- Do you know what data PayMe had on your employees? Can you evaluate it yourself?
- If not, how do you get the data from PayMe? If you can't get the data from PayMe for analysis, what information will you need?
- What information are you entitled to from PayMe under your contract?

If you are PayMe:

- How much are you telling your customers and when? Do you need help from your customers to validate impacted information?
- How do you manage the data review process with your customers' involvement (including document review)? How do you manage their expectations in relation to data review timeline?

Key Stumbling Blocks: Individual Notifications

If you are a PayMe customer:

- Who handles individual notifications?
- If you are not handling the notifications directly, how do you manage the recipients and content of the notifications?
- What do you say to your employees about the breach outside of these notifications?

If you are PayMe:

- Once you determine what you and your counsel believe to be required notifications, how do you communicate that to your customers? Do you, strategically, want to handle all individual notifications?
- What happens when a number of your customers have specific demands for the individual notification process?
- Are you entitled to indemnification from SendIT for the costs of notification?

Key Stumbling Blocks: Regulatory Notifications

If you are a PayMe customer:

- Do you want to make notifications to regulators, as required, yourself?
- If you allow PayMe to handle the regulator notifications itself, do you want to be named in the notification? How do you get comfortable that a regulator will know that you've fulfilled your obligation?
- What about your international regulators (e.g., supervisory authorities)?

If you are PayMe:

- Do you, strategically, want to handle any necessary regulator notifications on your own?
- If customers choose to make regulator notices themselves, how much involvement do you want in the language they use to describe the breach?
- How do you manage incoming regulator inquiries after notifications?

Questions & Contacts



Kirk Nahra

Partner
WilmerHale
@KirkJNahrawork
kirk.nahra@wilmerhale.com



Heidi Wachs

Managing Director
Stroz Friedberg, an Aon Company
@hlwachs
Heidi.Wachs@strozfriedberg.com



Shannon Togawa Mercer

Senior Associate
WilmerHale
@togawamercer
shannon.mercer@wilmerhale.com