

Third Party Risk Impact and Incident Response: *Cover all your Bases!*

Connie Mastovich, CISSP, CISA
Information Assurance Analyst
WellSpan Health
York, PA

The ABC's of Me

- **Hit the ground running in *Hospital IT*:** All facets of tech support, system maintenance, etc.
- ***Dabbled in Defense*:** IT Support for a local Defense Contractor
- ***Segued to Security*:** Northrop Grumman, Security support for a Top-Secret Air Force contract
- ***Sleep Sector Short Timer*:** Security and Privacy of sleep tracking devices at Philips Health Care
- ***Assessing and Analyzing*:** Small Data Security business, performed risk assessments across all industries along with ongoing remediation, education, etc.
- ***A Flash in Finance*:** Payment Card Industry (PCI) Audits for any organization processing payments
- ***Return to my Roots... but add Cybersecurity*:** Information Assurance Analyst at WellSpan Health. Third Party Risk Project lead along with a variety of other cyber security responsibilities

This Photo by
Unknown Author is
licensed under [CC BY-
SA](#)



Agenda

Proactive not Reactive

- Third Party Risk (TPR) in your Incident Response Plan (IRP)
- TPR in your Cyber Insurance Policy
- What about “their” IRP, Disaster Recovery Plan (DRP), etc.?
- Your role and responsibilities if a breach happens due to a third party




Ponemon Institute “The State of Cybersecurity and Third Party Remote Access Risk”

- 48% of organizations don't have comprehensive inventories of their third parties
- Third party attacks increased from 44% in 2021 to 49% in 2022
- Financial and Healthcare sectors are top targets for third party breaches
- Only 38% of organizations know what network access their third parties have
- 64% do not have an automated monitoring process of their third parties



VENDOR RISK MANAGEMENT

Things *Most* Organizations Know they *Should* be Doing
(with various levels of success...)

- Assess the risk of vendors
 - Identify significant risks
 - Determine possible mitigation steps
 - Using current risk appetite levels, decide on next steps
 - Monitor
 - Repeat at regular intervals
- Limit vendor access
- Centralized vendor repository 

Things *Most* organizations are just beginning to think about as it pertains to Third Party Risk



Things that make you go hhhmmm.....

Why the increase in third party breaches?

- The obvious answer is a poor security program: the lack of technical controls, insider risk, not enough security awareness training (or none?), access controls that are too loose, and on and on and on
- But... did you know that cybercriminals frequently compromise vendors of a company rather than the target itself **INTENTIONALLY**?



Your organization's cybersecurity controls are only as strong as the weakest link in your supply chain.



With ever-increasing numbers of third parties, it is extremely likely that your organization has vendors that do not meet your standards for security controls, regulations, or risk appetite.

INCIDENT RESPONSE PLAN: YOU KNOW YOU HAVE ONE, BUT ARE THIRD PARTY VENDORS APPROPRIATELY ADDRESSED?

Know Your Vendors

- Centralized Repository / Inventory
 - Contact information
 - Service Level Agreement (SLA) / Contract
 - Type and quantity of data accessed
 - Vendor assessment results
 - Internal business owner
 - Vendor Due Diligence Documents: More on this later

Table-Top Scenarios

- Include a third party compromise or breach as one of the exercises in your Incident Response Playbook
- If possible, have one of your current vendors actually take part
- Table-top tests should be a combination of internally developed scenarios and ones developed and delivered by an external partner/vendor
- Tests should vary in complexity and involvement



TPR and Cyber Insurance

Be sure that your policy includes third party liability insurance as well as first party liability

- First party coverage addresses data breaches that occur within your own network or systems
- Third party coverages protect your organization when a data breach occurs on a third party's network or systems, but includes your data
 - Media liability (covers libel, slander, and fraud)
 - Regulatory proceedings and fines
- Data Breach Insurance is only for the first party
- An effective third party risk management plan will have a positive impact on your cyber insurance rates

Third Party Due Diligence and Documentation



CYBER RISK

Third Party Vendor Risk is YOUR risk

- Vendor Assessments **must** include questions around:
 - Incident Response Plan
 - Disaster Recovery Plan
 - Business Continuity Plan
 - Operational Risk

A vendor without these plans in place puts your data at greater risk

It happened.....Your data was affected by a vendor breach. Now what?

- How did you find out? From the vendor or another method?
- Remove vendor access until further investigation takes place
- Initiate the Incident Response Plan and follow the steps already outlined
- Depending on the scope, the following entities should be involved:
 - Cyber Insurance Policy provider
 - Internal Legal counsel
- The determination of who is responsible for the following steps will not be made until more is known about the breach:
 - Breach notification
 - Media coverage
 - Potential Regulatory Agency involvement
- The more proactive you have been, the more protection you have



It's better to be prepared
than to get ready.

Will Smith

quote fancy



Resources

[Third-Party Incident Response Playbook – Tandem](#)

[The five W's of third-party incident management | Security Magazine](#)

[How to Handle Supply Chain Attacks, Ransomware and Other Incidents \(informationweek.com\)](#)

[New Guide: Third-Party Incident Response Playbook](#)

[Panorays](#)

[First-Party vs. Third-Party Cyber Liability Insurance | TechInsurance](#)

[How to manage third-party cybersecurity risks that are too costly to ignore | TechCrunch](#)

[15 Signs Your Vendor Has Been Breached in 2023 | UpGuard](#)



Connie Mastovich
cmastovich@wellspan.org
LinkedIn
Twitter: @ConnieGraceM
