

Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.



Clearwater

Healthcare – Secure, Compliant, Resilient

Monthly Cyber Briefing
September 2023



Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Cyber Briefings are eligible for HIMSS & CHIME CE credit
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

**HIMSS & CHIME
approved!**

2023 Monthly Cyber Briefings are now eligible for
HIMSS & CHIME certification CE credit

Agenda

- Cyber update
- Collaborating to Drive Strong Cybersecurity Program Governance
 - Governance Overview/Landscape
 - Intersection of Privacy + Security
 - Frameworks
 - Case Studies

September Speakers



Steve Cagle, MBA, HCISSP

Chief Executive Officer



Andrew Mahler, CHC, CIPP/US,
CHRC, CHPC

VP, Privacy & Compliance



Dawn Morgenstern, MBA, CHPC,
CCSFP

Sr. Director, Consulting Services, Chief
Privacy Officer



Cyber Update

Steve Cagle

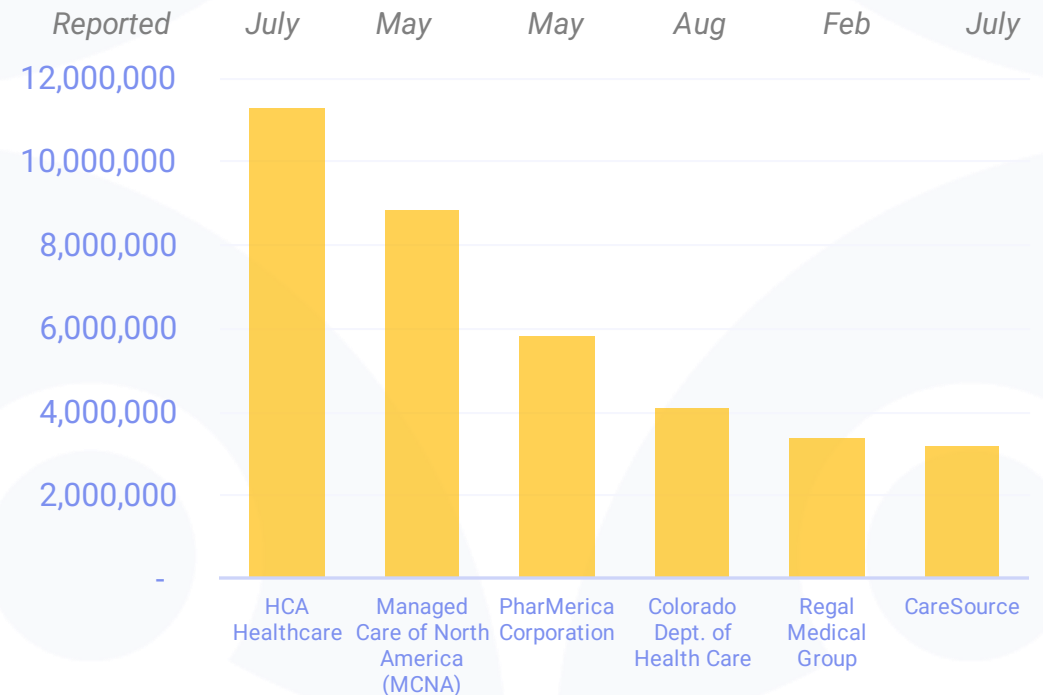
Healthcare Breaches Increasing in Total Due to Size

- 709 breaches and 74M records breached YTD 2023
- 78.6% increase in records breached
- 21.5m records reported breached in July 2023
- 10.5m records reported breached in August

Healthcare Records Breached



Top 5 Breaches of 2023



Prospect Medical Holdings Ransomware Attack

- August 3rd - 16 hospitals and 165 outpatient facilities
- 157th attack on U.S. Healthcare organization in 2023
- Rhysida ransomware group, known to target healthcare
- Waterbury Hospital systems recovered 28 days later

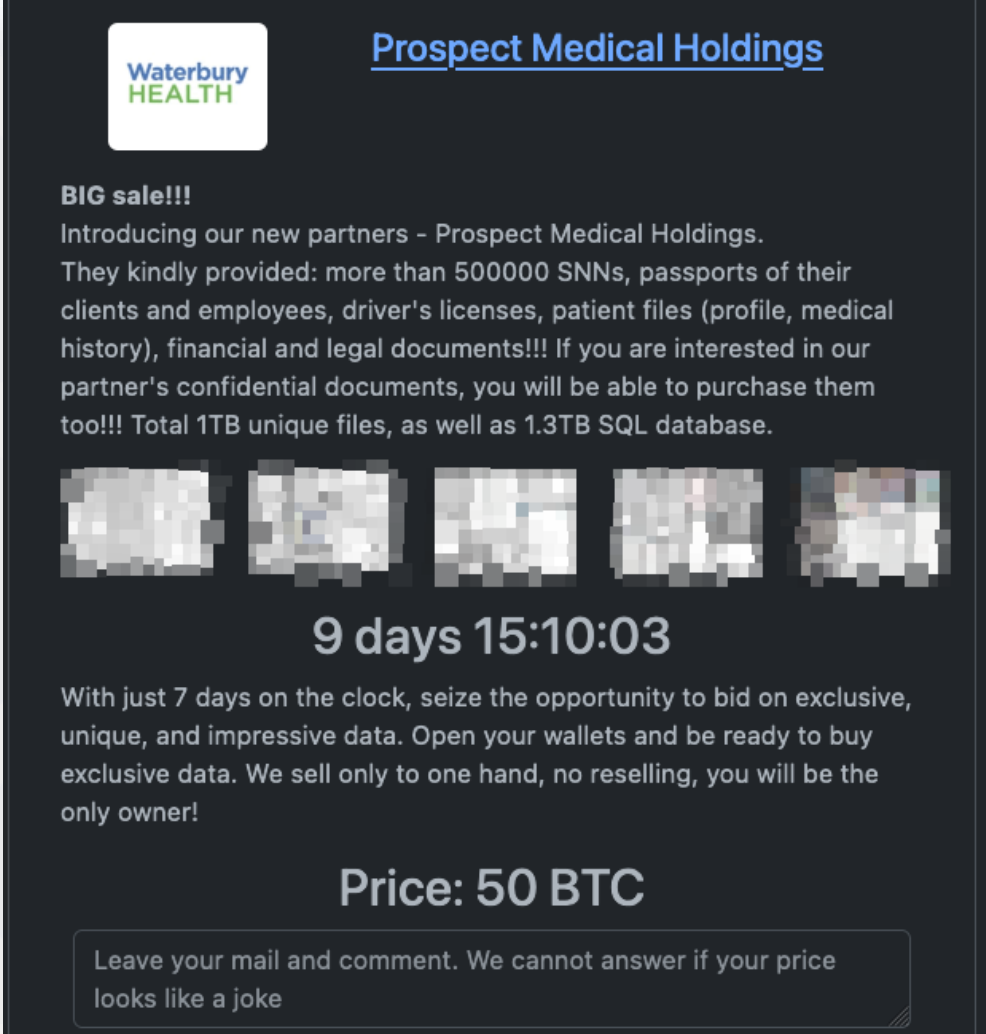
Critical Breach Detected - Immediate Response Required

Dear company, This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen - your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network. The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets. This could inflict significant reputational and financial damage. However, this situation is not without a remedy. Our team has developed a unique key, specifically designed to restore your digital security. This key represents the first and most crucial step in recovering from this situation. To utilize this key, visit our secure portal: [rhysidaf\[redacted\].onion](#) (use Tor browser) with your secret key [\[redacted\]](#) or write email: [\[redacted\]@onionmail.org](#) \ [\[redacted\]@onionmail.org](#) It's vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions. Time is a critical factor in mitigating the impact of this breach. With each passing moment, the potential damage escalates. Your immediate action and full cooperation are required to navigate this scenario effectively. Rest assured, our team is committed to guiding you through this process. The journey to resolution begins with the use of the unique key. Together, we can restore the security of your digital environment. Best regards

OK

Prospect Medical - 500,000 Records Stolen

- 8/25 – Over 500,000 records reported stolen including medical records, SSNs, passports
- Price of approximately 1.3m USD (50 Bitcoin)



Waterbury HEALTH

Prospect Medical Holdings

BIG sale!!!
Introducing our new partners - Prospect Medical Holdings. They kindly provided: more than 500000 SNNs, passports of their clients and employees, driver's licenses, patient files (profile, medical history), financial and legal documents!!! If you are interested in our partner's confidential documents, you will be able to purchase them too!!! Total 1TB unique files, as well as 1.3TB SQL database.

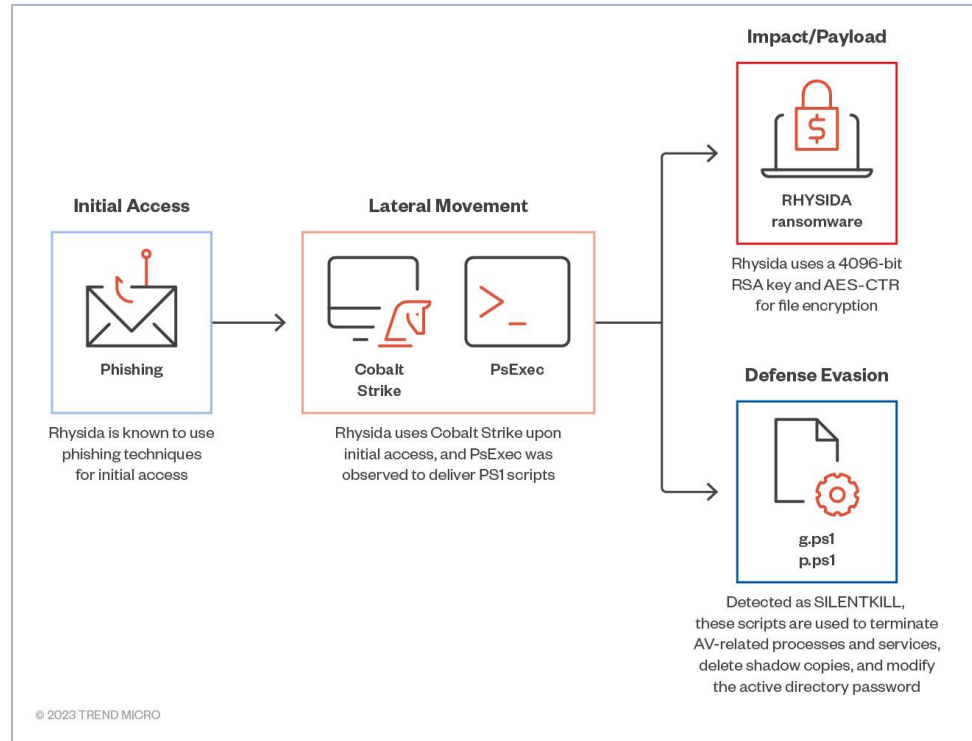
9 days 15:10:03

With just 7 days on the clock, seize the opportunity to bid on exclusive, unique, and impressive data. Open your wallets and be ready to buy exclusive data. We sell only to one hand, no reselling, you will be the only owner!


Price: 50 BTC

Leave your mail and comment. We cannot answer if your price looks like a joke


Rhysida Ransomware Group



Source: TrendMicro



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

August 4, 2023 TLP:CLEAR Report: 202308041500

Rhysida Ransomware

Executive Summary

Rhysida is a new ransomware-as-a-service (RaaS) group that has emerged since May 2023. The group drops an eponymous ransomware via phishing attacks and Cobalt Strike to breach targets' networks and deploy their payloads. The group threatens to publicly distribute the exfiltrated data if the ransom is not paid. Rhysida is still in early stages of development, as indicated by the lack of advanced features and the program name Rhysida-0.1. The ransomware also leaves PDF notes on the affected folders, instructing the victims to contact the group via their portal and pay in Bitcoin. Its victims are distributed throughout several countries across Western Europe, North and South America, and Australia. They primarily attack education, government, manufacturing, and technology and managed service provider sectors; however, there has been recent attacks against the Healthcare and Public Health (HPH) sector.

Overview of Rhysida

First observed on May 17, 2023, following the emergence of their victim support chat portal, hosted via TOR (.onion), Rhysida describes itself as a "cybersecurity team" that aims to help victims highlight potential security issues and secure their networks. While not much is known about the group's origins or country affiliations, the name Rhysida is a reference to the Rhysida genus of centipede and is reflected as the logo on their victim blog. The TOR page also shows the current auctions and total number of victims. The group's website also serves as a portal for Rhysida-centric news and media coverage, as well as details on how to contact the group should journalists, recovery firms, or fans be inclined to do so.

Rhysida is a 64-bit Portable Executable (PE) Windows cryptographic ransomware application compiled using MINGW/GCC. In each sample analyzed, the application's program name is set to Rhysida-0.1, suggesting the tool is in early stages of development. A notable characteristic of the tool is its plain-text strings revealing registry modification commands.

Rhysida ransomware is deployed in multiple ways. Primary methods include breaching targets' networks via phishing attacks, and by dropping payloads across compromised systems after first deploying Cobalt Strike or similar command-and-control frameworks. Of note, a previous [HC3 product on Russian-speaking RaaS group, Black Basta](#), detailed how both threat groups, Black Basta and FIN7 (aka Carbanak/Cobalt Group/Carbon Spider), share a TTP in their employment of Cobalt Strike.

When Rhysida runs, one cybersecurity firm observed a process of getting output from the command line, which apparently scans the files, runs the "file_to_crypt" function, and if successful, changes the file extension to ".rhysida":

Source: HHS

HSHS Ransomware Attack

This attack is a reminder of the importance of developing and testing an Incident Response plan that includes communication procedures to employees and the public

August 27th

August 28th

August 29th

August 30th

September 1



Cyber attack begins

Employee calls a breach reporting organization asking if they know what's happening

Statement issued by HSHS that website and phone lines are down and apologizes for inconvenience

HSHS website reports a system wide outage effecting "virtually all systems"

CEO reports cyberattack and reassures public they are working to recover

New Threat Brief Available from HHS

- Multi-Factor Authentication (MFA): An Overview
- Smishing
- Unintended Consequences of MFA
- Attack Vectors
- Threats to the Health Sector
- Recommendation



Source: <https://www.hhs.gov/sites/default/files/multi-factor-authentication-smishing.pdf>

Recommendations Based on Current Threat Environment

- Vulnerability scanning should be performed on an on-going basis. Remediate high and critical vulnerabilities right away
- Employ virtual patching in the case that a patch is not available, or not practical to implement
- Update security awareness training to account for more smishing and more sophisticated social engineering attack techniques
- Ensure your risk analysis is asset-based and updated on an on-going basis as changes in your environment occur
- Ensure on-going monitoring of end-points and correlate data with logs and other sources, and leverage automation and process to escalate and investigate security incidents
- Test your security controls through security controls validation assessments
- Develop and test incident response plans, including at the executive level



Collaborating to Drive Strong
Cybersecurity Program
Governance

Andrew Mahler

Dawn Morgenstern

Questions to Consider

- When you hear the word "implement," what do you think of?
- Do you know who is ultimately responsible for cybersecurity policies and procedures? What about data privacy/protection compliance?
- Who or what is responsible for incident response? Who or what ultimately makes the decision about how your organization will respond to an incident?
- What messages are you sending to your teams about effective communication and collaboration? For example, how often do security and privacy leaders meet/collaborate?
- Which office(s) manages the budget for third-party assessments, audits, etc.?
- How are risks identified, tiered, and managed?

Governance Overview

- Policies and procedures
- Roles and responsibilities
- Risk management
- Training and awareness
- Auditing and monitoring
- Incident management/response
- Individual rights
- Third-party risk
- Document retention

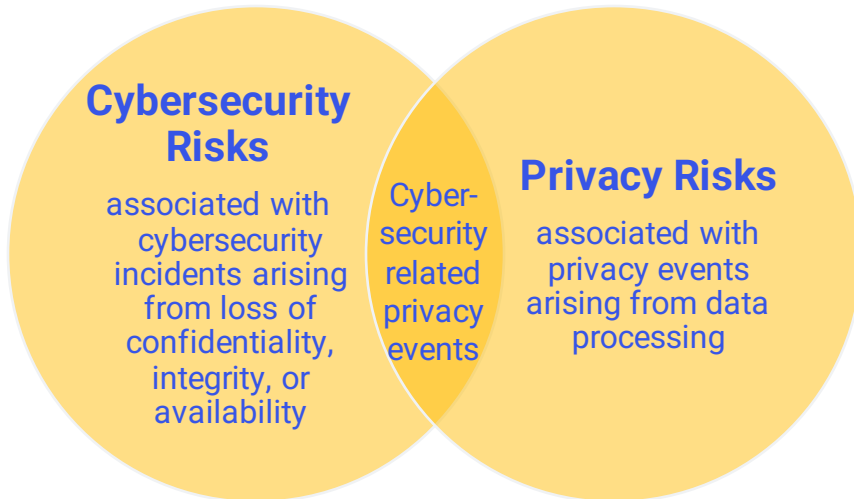


The Governance Landscape

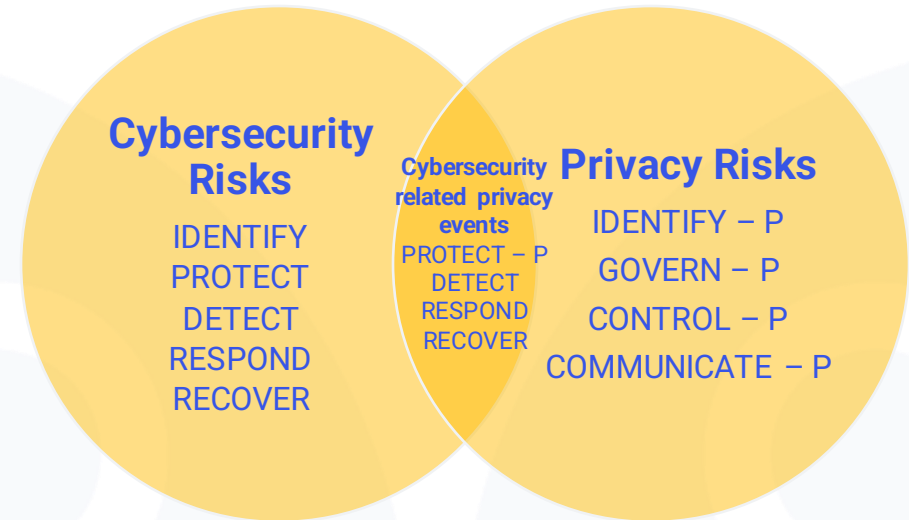
- **Challenges in Cybersecurity & Privacy Governance**
 - Rapid technological advancements
 - Evolving regulatory landscape
 - Bridging the gap between cybersecurity and privacy teams
- **Best Practices for Integrated Governance**
 - Clearly defined roles
 - Cross-functional collaboration and communication
 - Standardized policies and procedures across both domains
 - Regular training and awareness programs
 - Unified platforms
 - Third-party engagement

The Intersection of Privacy and Cybersecurity

- Consider privacy events as potential problems individuals could experience from system, product, or service operations
- Can have an adverse effect of data processing that organizations conduct
- The types of cybersecurity-related privacy events creates an overlap between privacy and cybersecurity risks
- Functions from NIST CSF and Privacy frameworks can be used in varying combinations
- The Protect-P Function overlaps for data protection to prevent cybersecurity-related privacy events and risk management
- The Cybersecurity Framework can be leveraged to further support Detect, Respond, and Recover functions

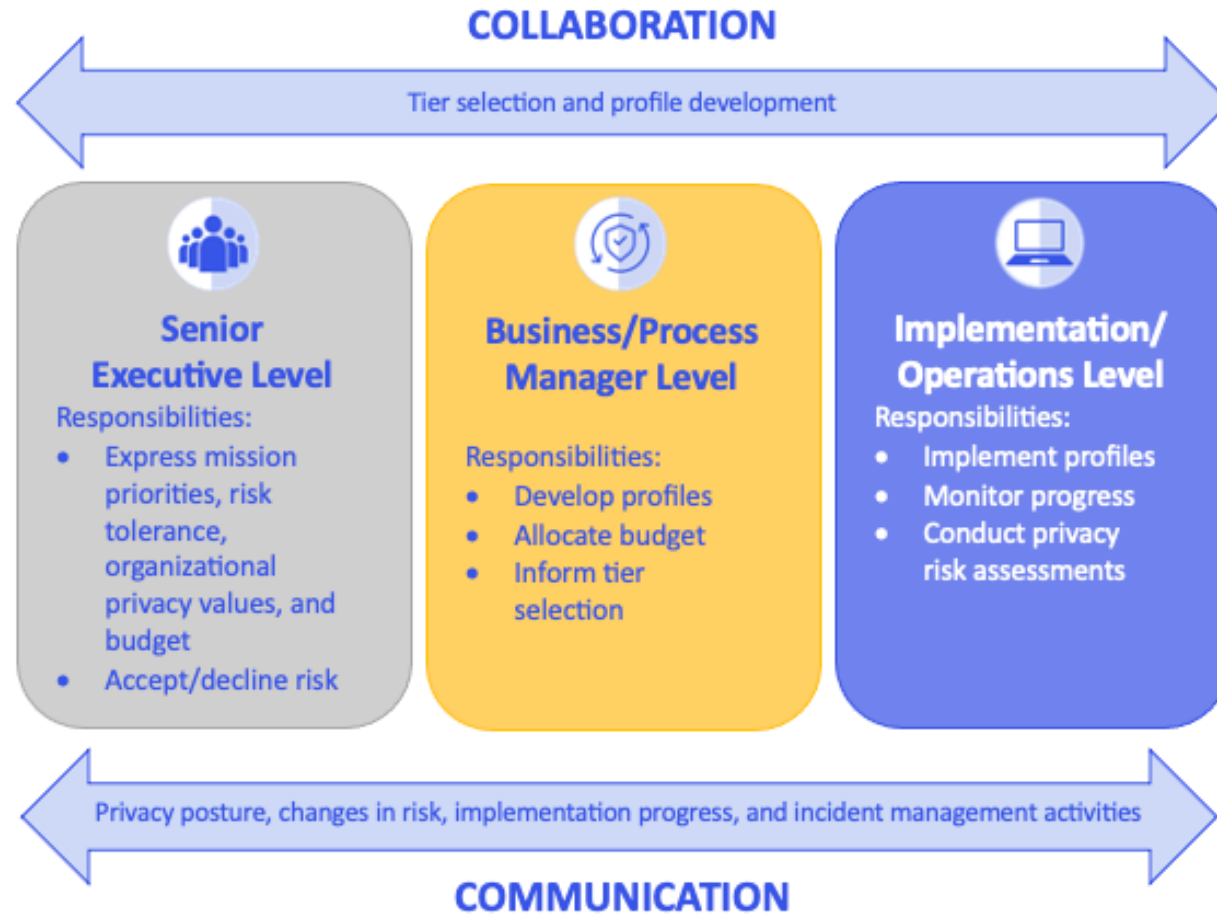


Cybersecurity and Privacy Risk Relationship



Using Functions to Manage Privacy Risk

Collaboration Example



Bi-directional Collaboration and Communication

Frameworks Can Help!

- **Frameworks: trends to combine data protection and cybersecurity frameworks**
 - Health Insurance Portability and Accountability Act (HIPAA)
 - General Data Protection Regulation (GDPR) and international laws
 - California Privacy Rights Act (CPRA) and state laws
 - NIST Special Publication 800-53
 - COBIT (Control Objectives for Information and Related Technologies)
 - ISO/IEC 27001 Information security management systems
 - 405(d) Health Industry Cybersecurity Practices (HICP)
 - Public Law 116-321
 - Others?

Case Example: Breach

Company: TechSolutions, a cloud-based service provider.

Situation:

The cybersecurity team at TechSolutions identified a potential security breach where customer data might have been exposed. They began an internal investigation but did not immediately inform the privacy office.

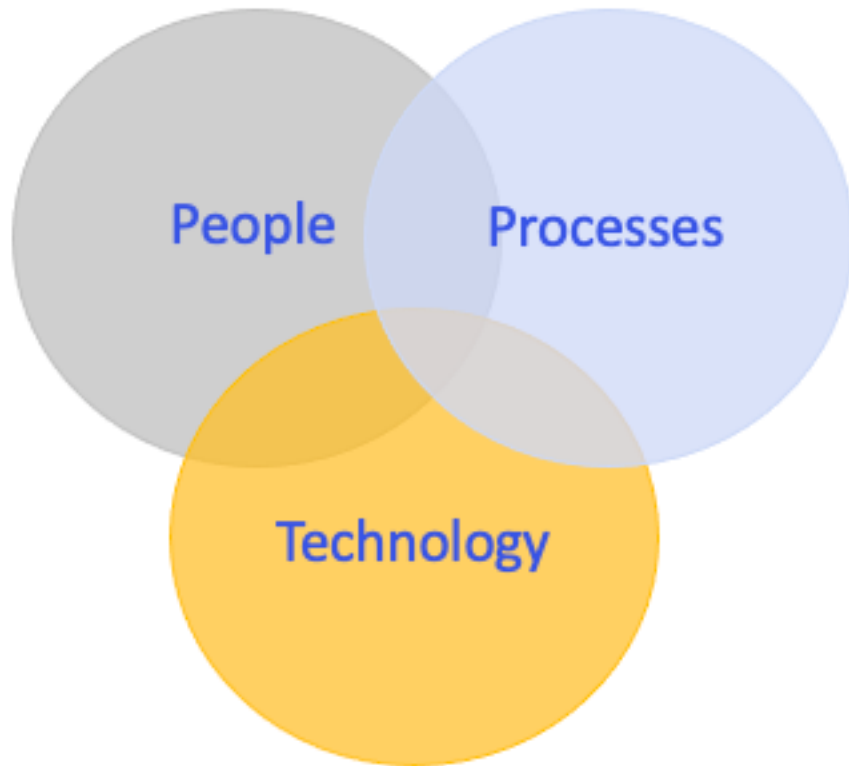
Outcome:

The privacy office was caught off-guard when customers began complaining after finding their data on the dark web. Because the privacy office was uninformed, they were not prepared to communicate effectively with affected customers, regulators, or the media.

Consequences:

- TechSolutions faced heavy fines for failing to notify affected parties in accordance with data protection regulations.
- The company's reputation suffered due to perceived negligence and lack of transparency.
- The lack of collaboration led to internal conflicts between the cybersecurity and privacy teams.

Holistic Approach



- It's a team effort - not just privacy or just security's responsibility
- Have a strategy and processes to continually monitor
- Educate senior leadership and your Board of Directors
- Ensure you have adequate resources
- Understand how changes to the regulatory environment may impact the way you do business
- Look at the regulatory requirements to determine where there are similarities
- Know what data you have and where your data lives (e.g., data mapping)
- Assess and remediate your risks
- Employ controls and technology to reduce your risk level

Parting Questions and Thoughts

- How can you affect leadership/management direction?
- How can you proactively address evolving threats and technological advancements?
- Are you communicating the value of collective insight and breaking down silos?
- If there are not clearly defined roles, how can you help develop a solution?
- Remember that there are tools, technologies, and people to support governance
 - Frameworks
 - Automation tools for policy enforcement
 - Incident management software
 - User access monitoring applications
 - Other colleagues and subject matter experts



Q&A

Steve Cagle

Andrew Mahler

Dawn Morgenstern



We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Upcoming Events



HIMSS Healthcare Cybersecurity Forum | September 7 - 8, 2023, Boston, MA



KLAS Research Digital Health Investment Symposium | September 12-13, 2023



Healthtech Leader 3.0 | September 27-29, 2023



■ Contact us

info@clearwatersecurity.com

www.clearwatersecurity.com

1.800.704.3394

