DEFENDING YOUR BUSINESS AGAINST CYBER THREATS:

Expert Strategies for Proactive Incident Response

September 19, 2023

RW TECHNOLOGY

HOGE · FENTON

XANTRION
CYBERSECURITY • IT SUPPORT

Moderator

STEPHANIE O. SPARKS
SHAREHOLDER – HOGE FENTON
(408) 947-2431
stephanie.sparks@hogefenton.com

Stephanie O. Sparks counsels companies on consumer privacy laws and helps them create and implement privacy and information security policies and incident response plans. Stephanie works with CISOs to conduct security assessments, provides privacy and data security awareness training, drafts HIPAA business associate and other agreements involving data protection, hosting, migration and transfer. When the inevitable breach happens, whether resulting from a stolen laptop, phishing scam or hacked server, Stephanie conducts the triage and manages all aspects of incident response, from investigation and computer forensics, media relations, notification, and remediation to negotiation and dispute resolution.

Panel Speaker

DANIEL ZBOROVSKI
PRINCIPAL CONSULTANT
RESTWELL TECHNOLOGY

- Over 25 years leading and mentoring security, technical, and programming teams
- Managed complex security projects across sectors including legal, healthcare, manufacturing, and professional services
- Conducted Cybersecurity risk reviews and GAP Assessments against key frameworks like SOC 2, HIPAA, ISO 27001, NIST 800-53, and CMMC
- Serves as a fractional CISO for a diverse range of organizations, including healthcare providers, public companies, financial institutions, and medical device manufacturers, offering specialized, high-level cybersecurity strategies and guidance
- Expertise in creating, updating, and testing Incident Response Plans tailored to specific industry requirements and compliance frameworks
- Proven track record of conducting tabletop exercises and real-world simulations to validate IRP effectiveness

RW TECHNOLOGY

HOGE · FENTON

XANTRION
CYBERSECURITY • IT SUPPORT

Panel Speaker

CHRISTIAN KELLY, CISSP
CHIEF TECHNOLOGY OFFICER
XANTRION

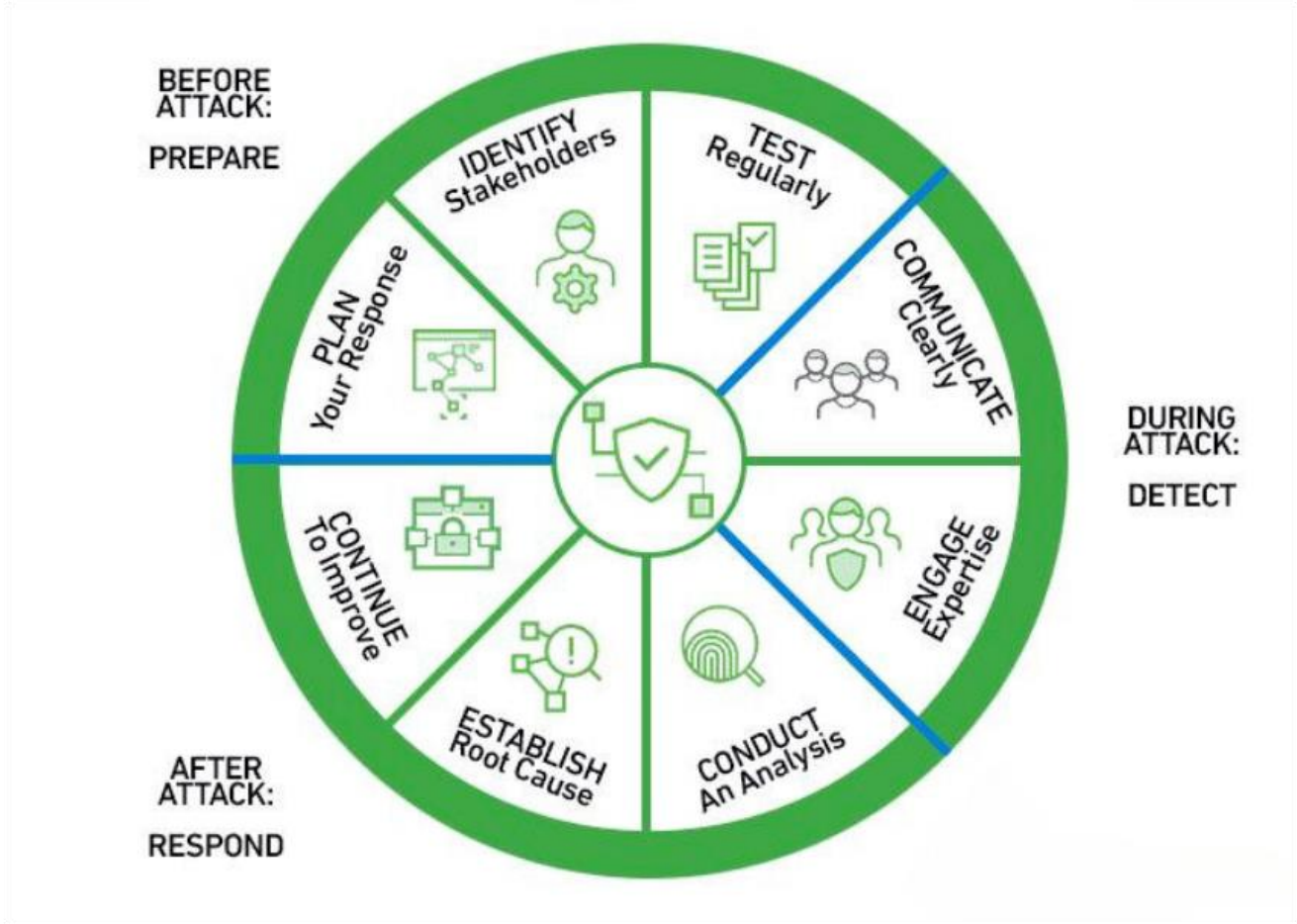
- Certified Information Security Professional (CISSP)
- 22 years of IT experience
- Xantrion CTO for 7 years
- Responsible for ensuring the availability and security of client systems as well as conformance to regulatory requirements
- Point person for Xantrion and client security incidents

RW TECHNOLOGY

HOGE · FENTON

XANTRION
CYBERSECURITY • IT SUPPORT

What is a Cybersecurity Incident Response Plan (IRP)?



RW TECHNOLOGY

HOGE · FENTON

XANTRION
CYBERSECURITY • IT SUPPORT

What a Cybersecurity IRP is Not!

1. Not a replacement for prevention
   - Incident response plans complement preventative measures like multifactor authentication and security awareness training; they don't replace them.
2. Not Just a Technical Problem
   - It involves coordination across multiple departments including legal, PR, and human resources.
3. Not Just for IT
   - While the IT department often leads incident response, every employee has a role to play in identifying and reporting potential incidents.
4. Not a One-Size-Fits-All Solution
   - Incident response plans should be tailored to the specific organization and its unique risks and vulnerabilities.

Why Do I Need One?

1. Be more resilient in the face of the increasing cyber threat landscape
   - 58% of data breaches take place at small and medium businesses
   - Ransomware is responsible for about 1 in 3 breaches in small and medium businesses
2. Reduce the cost of cybersecurity incidents
   - The average cost of a data breach in small and medium businesses is $3.31 M
   - Organizations with high levels of incident response planning saved $1.49 M
3. Reduce downtime
   - Organizations with high levels of incident response planning resolved incidents 54 days faster
4. Regulatory compliance
   - In many industries, having a documented incident response plan is a legal requirement. Failure to comply can result in financial and legal penalties
   - Frameworks such as: HIPAA, PCI-DSS, FINRA, SEC, CPRA, SOX, CMMC and GLBA require an incident response plan
5. Cyber Liability Insurance Coverage
   - Many cyber insurance policies will require you to have an incident response plan in place. Without one, you may be ineligible for coverage or receive less favorable terms

2023 Data Breach Investigations Report, Verizon and Cost of a Data Breach Report 2023, IBM

RW TECHNOLOGY

HOGE · FENTON

XANTRION CYBERSECURITY • IT SUPPORT

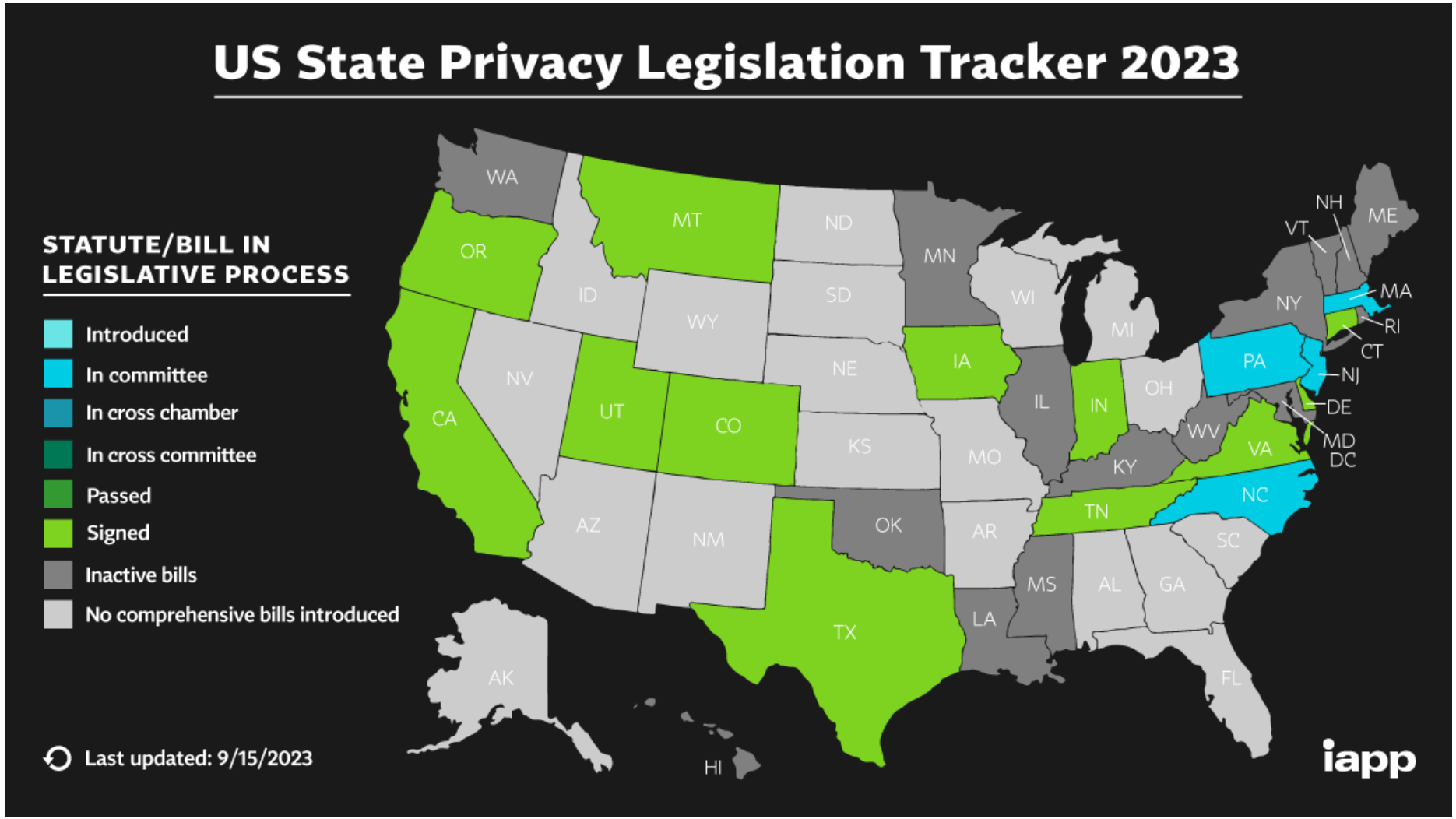
PREPARE: How to Develop an Effective IRP

1. Initial Risk Assessment
   - Evaluate your organization's current risk profile, data assets, and infrastructure vulnerabilities
   - This will set the groundwork for the scope of your plan
2. Stakeholder Engagement
   - Involve key stakeholders from legal, HR, IT, and executive teams early in the process
   - This ensures the plan aligns with organizational objectives and compliances
3. Define Incident Categories
   - Classify types of incidents your organization is most likely to encounter
   - The response procedures will vary depending on the severity and type of incident
4. Legal & Regulatory Alignment
   - Ensure the plan is compliant with relevant laws, regulations, and industry standards
   - Update the plan regularly to account for legislative changes
5. Develop Partnerships with External Experts
   - Identify and establish relationships with external experts who can provide specialized skills or resources that your internal team lacks.

PREPARE: How to Update and Test Your IRP

1. Gap Analysis
   - Conduct a comprehensive review of your organizations risks, and existing plan to identify gaps, weaknesses, or areas for improvement
2. Regulatory Alignment
   - Ensure your plan is in sync with the latest legal and regulatory requirements, such as HIPAA, CPRA, or SEC cyber rules.
3. Tailored Updates
   - Customize the existing plan based on your unique organizational structure, technical environment, and business objectives.
4. External Expert Assessment
   - Evaluate existing expert partnerships and recommend additional experts to close skill or resource gaps in your incident response capability.
5. Real-world Simulation
   - Develop and execute real-world incident simulation exercises to evaluate the plan's effectiveness under stress.
6. Employee Training
   - Conduct tailored training sessions and workshops for your incident response team and relevant staff members.

LEGAL: Federal & State Laws



Source: https://iapp.org/media/images/resource_center/State_Comp_Privacy_Law_Map.png

RW TECHNOLOGY

HOGE · FENTON

XANTRION CYBERSECURITY • IT SUPPORT

LEGAL: Complex Notification & Reporting

How to ensure your IRP complies with laws and regulations like CPRA & SEC cyber rules

Groups of State(s)	Timing for Indiv. Notice	Whether you must report to AG, etc.
Alabama	45 days	Only if 1,000
Arizona	45 days	Only if 1,000
California	Most expedient time possible	Only if 500
Colorado	30 days	Only if 500
Florida	30 days	NO
Kansas	"reasonable time"	NO
Kentucky	"reasonable time"	NO
Maryland	45 days	YES – MUST REPORT TO STATE PRIOR TO NOTIFYING INDIVIDUALS
Montana	"reasonable time"	YES **(MUST NOTIFY AND REPORT SIMULTANEOUSLY)**
New Jersey	"reasonable time"	YES - MUST REPORT TO STATE POLICE PRIOR TO NOTIFYING INDIVIDUALS
New York	"reasonable time"	YES – plus NY State Police and NY Dept of State
North Carolina	"reasonable time"	YES
Ohio	45 days	NO
Washington	30 days	Only if 250

RW TECHNOLOGY

HOGE · FENTON

XANTRION CYBERSECURITY • IT SUPPORT

LEGAL: Attorney-Client Privilege, Work Product

- Attorney-Client Privilege, Fed. R. Evid. 502; Cal. Evid. Code §§ 915, 954-955
- Attorney Work-Product Doctrine, Fed. R. Evid. 502; Cal. Evid. Code § 915

RESPOND: Include Recovery & Investigation in IRP

1. Understand business priorities
   - Assess priorities of recovering the business quickly vs. insurance providers and forensics priorities. They don't always coincide.
   - Perform an impact business analysis to understand your critical systems an impact of downtime
2. Plan Communication Protocols
   - How will communication happen if email or internal messaging is compromised? Having a pre-established, secure channel for incident communication can be valuable for timely response and recovery.
3. Test recovery capabilities
   - Don't wait for an incident to test recovery or backups and replication. Part of your IRP should include validation and testing of backups and replication.
4. Perform tabletop exercises
   - Insurance will be a large part of any response and will dictate both vendors and procedures. Understand their requirements early and try to include them in an exercise.
   - Tabletop exercises are meant for uncomfortable questions and changes to the plan. It's not a pass/fail exercise

DETECT: Include Detection & Containment in IRP

1. Plan should call for capabilities and technologies which are needed to determine impact and speed analysis
2. Early detection and containment
   - Most attackers are on networks and systems for weeks or months before fully executing their attacks
   - Although attackers use stealth, they can trigger small clues which a SOC can pick up on if the signal to noise ratio isn't too high
3. Realtime containment capabilities
   - Ability to isolate systems or networks which are suspected of a breach quickly to prevent larger impact
4. Logging considerations for forensic investigation

Cybersecurity IRP Take Aways

1. For those without IRP
   - **Cost of Inaction**
     - Not having an IRP can result in significantly higher recovery costs as well as legal and regulatory repercussions
   - **Resource Allocation**
     - Without an IRP, your organization may not have the necessary resources or procedures in place, which lead to a chaotic and ineffective response
2. With IRP
   - **Regular Tabletop Exercises**
     - The effectiveness of an IRP is only as good as its execution. Regularly scheduled tabletop exercises with key stakeholders can identify gaps in your plan and improve incident readiness
   - **Alignment with Regulatory Frameworks**
     - Continuously align your IRP with evolving compliance requirements and industry best practices. This not only ensures legal protection but also keeps your plan updated against emerging threats.

Questions?

Thank You for Attending

STEPHANIE SPARKS
SHAREHOLDER/FOUNDER
Privacy & Data Security
Hoge Fenton
1-408-947-2431
stephanie.sparks@hogefenton.com

DANIEL ZBOROVSKI
PRINCIPAL CONSULTANT
Restwell Technology

CHRISTIAN KELLY, CISSP
CHIEF TECHNOLOGY OFFICER
Xantrion

Contact Us

Additional Questions or need to request MCLE credit?

(Please include CA Bar Number)

email webinars@hogefenton.com

HOGE FENTON