lightstream

5 THINGS YOUR BREACH RESPONSE ATTORNEY NEEDS YOU TO KNOW BEFORE AN INCIDENT OCCURS

A blueprint of actionable steps you can take to ensure your prepared incidence response plan will be effective should an incident occur.

LIGHTSTREAM
208 N 2100 West, Suite 200
Salt Lake City, UT 84116
Phone: 877-95-LIGHT

Follow us on

Let us tell you more about
the amazing things we do.

RANSOMWARE TARGETS ORGANIZATIONS OF ALL SIZES

Confidence in cloud infrastructure and platform services (CIPS) security continues to grow. “Cloud-first” strategies are now common, even among risk-averse organizations; however, execution remains impeded by a lack of necessary skills and tools to ensure secure deployment. In a recent Gartner survey, the most commonly cited challenge to cloud adoption was gaining security team approval and support for cloud migration strategies, suggesting that security teams are struggling to adapt to increasingly complex cloud technologies.

To make matters worse, Ransomware tactics and techniques continued to evolve in 2021 as well. Threat actors’ growing technological sophistication brought them lucritive returns by employing ransomware-as-a-service (RaaS), even going so far as to assist victims with payments via 24/7 help centers!

Ransomware developers targeted cloud infrastructures to exploit known vulnerabilities in cloud applications, virtual machine software, and virtual machine orchestration software. Ransomware threat actors also targeted cloud accounts, cloud application programming interfaces (APIs), and data backup and storage systems to deny access to cloud resources and encrypt data. In addition to exploiting weaknesses to gain direct access, threat actors sometimes reach cloud storage systems by compromising local (on-premises) devices and moving laterally to the cloud systems. Ransomware threat actors have also targeted cloud service providers to encrypt large amounts of customer data.

TOOLS

Cloud networking has enabled companies to be more nimble, and provide better end user experiences. However, security and response protocols must be implemented and monitored

PEOPLE

Employees are the frontline security of an organization and should be educated in security principles and actions. Hosted and cloud-based managed services provide increased protection

CULTURE

FinOps increases the business value of cloud by bringing together technology, business and finance professionals to deliver faster while gaining financial and operational control

THE RANSOMWARE LIFECYCLE

PHISHING EMAILS, RDP EXPLOITATION, AND EXPLOITATION OF SOFTWARE VULNERABILITIES REMAIN THE TOP THREE INITIAL INFECTION VECTORS, AND ARE INCREASING.

01 | INITIAL DISCOVERY

02 | BASIC INTEL + ACTIVATE IR PLAN & TEAM

03 | SECURITY EXPERTS

04 | SECURITY EXPERTS

05 |DATA RECOVERY + RESTORATION

06 | FORENSIC EXAMINATION

07 | INCIDENT OR BREACH?

08 | AFTER ACTION REVIEW

09 | MOST COMMON CAUSES

70%

of all enterprise workloads will be deployed in cloud infrastructure and platform services by 2023, up from 40% in 2020

>99%

of cloud breaches will have a root cause of preventable misconfigurations or mistakes by end users through 2025

AN INCIDENT HAS TAKEN PLACE. WHAT DO YOU DO NEXT?

1. Understand that properly investigating and responding to an incident is not optional, in most cases, and will be required by some source of law or regulation. This makes it a legal issue. While we are talking law, also understand:
   - What a "privilege" is and is not, and
   - The difference between "incident" and "breach".
2. Cyber insurance—you must have it—trust me.
3. It takes a team—while you must have a "head coach" and someone must own the IR process, to address all the objectives, you must have a full team in place, internally and externally.
4. Your team must be trained, prepared, and eligible to play on game day.

Incident or Breach experienced

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that jeopardizes the confidentiality, integrity, or availability of information resources or operations.

Hour 1

- Initial discovery
- Basic intel
- Activate IR Plan and IR Team
- Triage security and backups
- <u>Do not</u> wipe drives
- Start preserving evidence
- Don't communicate with TA

>12 Hours

- Notify insurance carriers
- Engage security experts
- Engage data recovery experts
- Report to law enforcement
- Notify employees
- Notify key business partners
- Begin data recovery and restoration
- Confirm not obvious "Breach"

12–72+ Hours

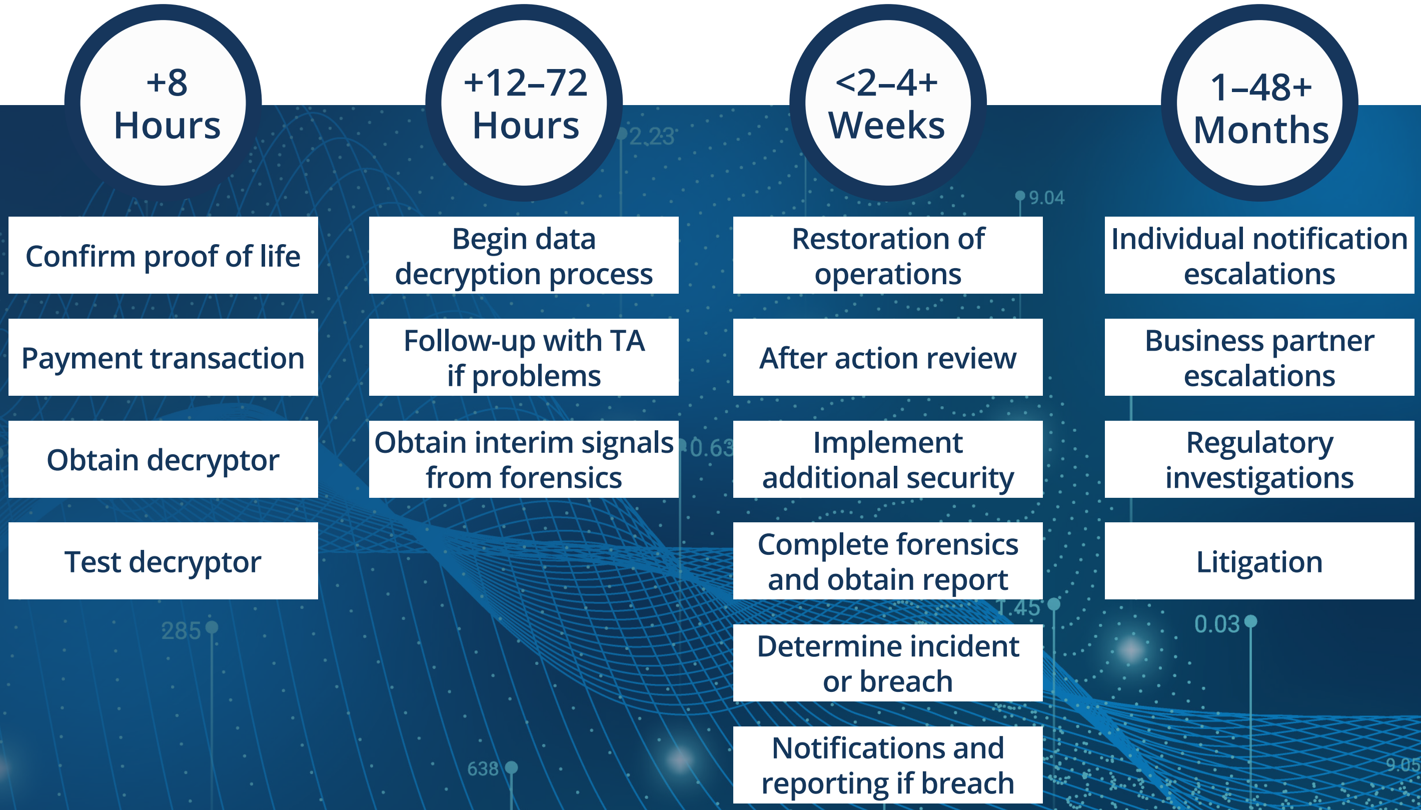
- Implement interim security
- Negotiate with threat actor
- OFAC clearance
- Carrier approval for payment
- Begin forensics
- Plan for PR and potential notification

lightstream

- Approval of your players—external vendors and cyber insurance.
- Education and training.
- Tabletops—your scrimmage games.

5 The most functional "real world" Incident Response Plan may very well be a whiteboard image from a brainstorming or tabletop session.

A managed services partner is key in delivering controlled, compliant and economical cloud strategies, therefore keeping the organization competitive.



+8 Hours	+12–72 Hours	<2–4+ Weeks	1–48+ Months
Confirm proof of life	Begin data decryption process	Restoration of operations	Individual notification escalations
Payment transaction	Follow-up with TA if problems	After action review	Business partner escalations
Obtain decryptor	Obtain interim signals from forensics	Implement additional security	Regulatory investigations
Test decryptor		Complete forensics and obtain report	Litigation
		Determine incident or breach	
		Notifications and reporting if breach	

About Shawn Tuma, Partner, SpencerFane

Shawn Tuma helps businesses protect their information and protect themselves from their information. He represents a wide range of clients, from small to midsize companies to Fortune 100 companies, across the United States and globally in dealing with cybersecurity, data privacy, data breach and incident response, regulatory compliance, computer fraud related legal issues, and cyber-related litigation.

Having practiced in this area of law since 1999, Shawn is widely recognized in cybersecurity and data privacy law. He is frequently sought out and hired by other lawyers and law firms to advise them when these issues arise in cases for their own clients.

Shawn's practice covers: Cyber Risk Management, Cyber Incident Response, Cyber Security, Hacking, and Data Breach Litigation

About Rafal Los, VP of Security Strategy, Lightstream

Raf has a real interest in pushing the envelope. He is a recognized security expert with 20+ years' experience working inside companies from the Fortune 10 to a firm of less than 10. His weekly podcast Down the Security Rabbithole has over 25K listeners per month. At Lightstream, Raf leads the security business and is responsible for strategy and development of security products and services. He is also an active member of the Security Advisor Alliance, serving on the advisory board with the intent of creating innovative ways for security leaders to give back to their communities through service and knowledge sharing.

For a one-on-one consultation to discuss how to ensure your cloud is secure, contact us now.

5 Things Your Breach Response Attorney Needs You To Know Before An Incident

Connect | Protect | Optimize

Sponsored by:

Need a refresher?

Click the icon to the left to be taken to the on-demand webinar.