Executive Roundtable Series

Sponsored by SpyCloud

Timeline of a Breach: How to Improve Detection and Response

Hosted by

Chip Witt - *Head of Product Strategy, SpyCloud*
Nick Holland - *Director, Banking and Payments, ISMG*

Agenda

6:00pm - Registration, Networking
6:30pm - Introductions and Opening Remarks
6:45pm - Roundtable Discussion
8:30pm - Program Conclude

SpyCloud

iSMG
INFORMATION SECURITY
MEDIA GROUP

Introduction

As the Verizon Data Breach Investigations Report reminds us each year, when breaches are successful, the compromise can be measured in minutes or even seconds. But detection and response times? Too often those are measured in weeks or months.

What are 2020's latest breach trends, including targeted attacks and third-party threats? What does a third-party breach have to do with the security of your organization? How are attackers using breach data for maximum damage? What can you do to speed up detection and response?

This exclusive executive roundtable on **Timeline of a Breach: How to Improve Detection and Response** will provide answers to these and other questions.

Guided by insights from Chip Witt, head of product strategy at event sponsor SpyCloud, this invitation-only dinner will also draw upon first-hand experience and new research, as well as from the experiences of the attendees, who will share their views on how they have come to better understand and respond to breach trends and timelines. Among the discussion topics:

- What are today's top breach trends, including both targeted and untargeted attacks?
- What type of threat intelligence is most effective in detecting and preventing breaches?
- Which strategies and tools can be employed to minimize and mitigate the third-party threat?

You'll have the opportunity to discuss the topic with a handful of senior executives and market leaders in an informal, closed-door setting, from which you will emerge with new strategies and solutions you can immediately put to work.

Discussion Points

Among the questions to be presented for open discourse:

- What types of attacks – targeted or untargeted – are of greatest concern to you and your organization today?
- Where are your biggest gaps in detection? Response?
- What type of threat intelligence is most effective in detecting and preventing breaches?
- Which strategies and tools have you employed to minimize and mitigate third-party threats?
- What will you do this year to improve your times to detect and respond?

About the Expert

Joining our discussion today to share the latest insights and case studies:

Chip Witt

Head of Product Strategy, SpyCloud

Witt has nearly 20 years of diverse technology experience, including product management and operations leadership roles at Hewlett Packard Enterprise, Webroot, VMware, Alcatel and Appthority. As head of product strategy at SpyCloud, he manages the customer success program, which provides cloud-based security services to help businesses of all sizes prevent data breaches and account takeover attacks by alerting when employee or company assets have been compromised. He works closely with field intelligence teams specializing in OSINT and HUMINT tradecraft, actor attribution and underground monitoring.

About SpyCloud

SpyCloud is the leader in account takeover (ATO) prevention. We strive to help businesses of all sizes mitigate account takeover by proactively remediating account exposures for their employees and customers in an automated way. We accomplish this through our award-winning ATO prevention solutions powered by a world-class team of security researchers and technology.

For more information, please visit https://spycloud.com/.

About the Moderator

Leading our discussion today is:

Nick Holland

Director Banking and Payments, ISMG

Holland, an experienced security analyst, has spent the last decade focusing on the intersection of digital banking, payments and security technologies. He has spoken at a variety of conferences and events, including Mobile World Congress, Money2020, Next Bank and SXSW, and has been quoted by The Wall Street Journal, CNN Money, MSNBC, NPR, Forbes, Fortune, BusinessWeek, Time Magazine, The Economist and the Financial Times.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from the North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Q&A WITH THE EXPERT

Timeline of a Breach: How to Improve Detection and Response

In advance of this event, ISMG's Tom Field spoke about breach detection and response with subject matter expert **Chip Witt**. Here are excerpts of that conversation.

Chip Witt

Head of Product Strategy, SpyCloud

SpyCloud

Top Concerns

NICK HOLLAND: What are the breach trends that most concern you as we start 2020?

CHIP WITT: There are several, namely:

The increasing risk of third-party ATO/suppliers and vendors being targeted: This is a trend that we started hearing about all the way back in 2014, when Target acknowledged that they were breached through a supplier, and it hasn't slowed down (even Equifax blamed their breach on a third party). Ponemon Institute's third annual "Data Risk in the Third-Party Ecosystem" study found that 59 percent of respondent companies experienced a data breach caused by a third party or vendor. Think about all the third parties who have access to just your financial, HR, and marketing systems housing sensitive IP, PII and customer data, and it's easy to understand the scope of the risk your vendors pose and the implications of a breach caused by a third party.

The increasing use of ransomware: Based on an increasing number of incidents in 2019, we saw bad actors deploy ransomware technology to target public infrastructure. Louisiana's governor declared a state of emergency following a vicious ransomware campaign that targeted the state's systems, and throughout the year, attackers focused on government infrastructure, hospitals and schools - exactly the kind of businesses that underinvest in cybersecurity protections. Here is a good breakdown of ransomware related stats.

The effects of GDPR might induce enterprises to pay criminals rather than fines: While it's not really possible to track, it's easy to imagine that strict rules might force some entities to succumb to paying criminals rather than telling authorities. Will it become more sensible to pay a $1 million ransom to a bad actor rather than $10 million in GDPR fines and dealing with the negative PR? It's a strategy unlikely to pay dividends, but it could tempt smaller, less sophisticated organizations.

The Damage

HOLLAND: Where – and when – do you see the most damage being done to breached organizations?

WITT: We're seeing security teams underestimate the damage caused by manual, targeted attacks performed by sophisticated cybercriminals (as opposed to brute-force credential stuffing attacks performed by bots), which take place at the beginning of the breach timeline. Customers on our advisory board told us recently that targeted attacks account for 80 percent of their overall loss, while untargeted, credential stuffing type attacks accounting for the other 20 percent.

> **"Will it become more sensible to pay a $1 million ransom to a bad actor rather than $10 million in GDPR fines and dealing with the negative PR?"**
>
> Chip Witt, SpyCloud

During this time - the first 18-24 months after the breach takes place - criminals do their best to monetize the data in a variety of creative ways. Tactics may include:

- "Fingerprinting" an organization to identify defense thresholds;
- Combining manual checks and specialized tools like purplespray to systematically test password variations without raising alarms;
- Bypassing MFA via phishing, social engineering, man-in-the-middle attacks, iCloud vulnerabilities or session hijacking;
- Thwarting SMS-based 2FA with SIM-swapping, phone porting or exploiting vulnerabilities in cell infrastructure (SS7 network);
- Searching compromised email and storage accounts for TOTP seed backups or photos to use for authentication;
- Leveraging extortion, blackmail and social engineering.

Who are the targets of these attacks? Potential high-value victims include wealthy or high-profile individuals, C-level executives and developers, due to their level of systems access.

Detection, Response Times

HOLLAND: What are your insights on detection and response times?

WITT: Given targeted attacks leveraging breached data are performed by sophisticated attackers far earlier than knowledge that those breaches have occurred reaches the mainstream, and those attacks account for 80 percent of enterprise losses, we believe building a security program around technologies that proactively leverage data acquired through HUMINT tradecraft very early in the breach timeline is a critical path to success.

> **“We’re seeing security teams underestimate the damage caused by manual, targeted attacks performed by sophisticated cybercriminals.”**
>
> Chip Witt, SpyCloud

Detecting and responding to a threat is as much about looking in the right place at the right data in a timely manner as it is about responding swiftly. If you are responding quickly to inadequate information, you’re not really solving anything.

Automation is key. Even with the very best data, if you are not enabling adept response through automated operationalization (e.g. relying on humans collecting and applying intelligence), something will eventually be missed, especially at scale. Our customers continue to tell us that success hinges both on access to great data and in being able to make that data operationally actionable through automation.

Misconceptions

HOLLAND: What is most misunderstood about the timeline of a breach?

WITT: The idea that credential stuffing is the thing you need to worry about. Stolen credentials being widely available to criminals is a worrisome concept, not to mention crimeware tools that are easy to use for even unsophisticated criminals to monetize that data (i.e. account checkers). But credentials are leaked to the dark web and sold/traded on public forms years after the breach takes place. By then, most users will have changed their passwords, which is why credential stuffing has only a 0.2 pecent to 2 percent success rate. Not to downplay the effect that can have, but the damage that is done at the beginning of the timeline (that first 18-24 months) is what's underestimated and misunderstood. It's what we're here to demystify.

HOLLAND: How can organizations best improve their times to detect and respond?

WITT: As above, better operationally actionable data and automation.

> **"If you are responding quickly to inadequate information, you're not really solving anything."**
>
> Chip Witt, SpyCloud

SpyCloud's Role

HOLLAND: How is SpyCloud helping enterprises shrink that time to discover and minimize breach impact?

WITT: SpyCloud is focused on proactively preventing breaches and online fraud caused by account takeover. This is done by identifying when employees' or customers' credentials have been exposed in the underground and helping drive appropriate remediatory action (e.g. forcing a customer visiting an e-commerce site down an alternate identity validation path before a transaction is allowed to be completed, or forcing an employee to reset an exposed password in Active Directory). ■

Notes

Notes

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® Just for Credit Unions GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk® TODAY CAREERS INFO SECURITY® ~~Data Breach~~. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io