FINSBURY GLOVER HERING | MANDIANT

SILENCE IS NOT GOING TO HELP

Preparation is critical before a cyber attack: Part two in a conversation with Mandiant

AUGUST 2021

CYBERSECURITY GLOBAL CONVERSATION SERIES

As with any type of crisis, organizations that plan, prepare and train ahead of time are going to be better positioned to respond effectively. And that certainly goes for cybersecurity as well. Most notably, identifying the cross-functional working group that will be responsible for managing a cyber issue is critical for proper prevention, detection and remediation.

In the latest installment of Finsbury Glover Hering's global cybersecurity conversation series, Global Managing Partner Paul Holmes and Managing Director Mike Dolan spoke with Manny Jean-Georges, Manager, and Brice Daniels, Director, at Mandiant Consulting, a leading provider of incident response, strategic readiness, technical assurance and security training services. The following is part two of a two-part series in this conversation and has been edited for length. Part one can be found here.

Mike: Looking ahead, what cyber threats are companies not thinking about right now that you guys think they should be focused on?

Manny: If there's one thing the last few months have shown us, it's that supply chain-type attacks are something organizations need to be aware of. Understanding attacker sophistication in this area and in turn thinking about an effective plan for how to prepare and react is critical.

Brice: Malware, including early ransomware, has also evolved from what it was five years ago. It has evolved into an increasingly effective business model based primarily on ransomware and extortion attacks. What this means is that organizations can't ignore even some of the more trivial, commodity malware, because while trickbot, for instance, could simply be there to steal your credentials, it could also be there as the precursor to a larger enterprise ransomware attack.

Paul: I know that you both work with communications teams when you're managing an incident and investigating. What are the top one or two things that you like your partners in communications to understand and keep in mind in situations like these?

Brice: I think one of the biggest problems is that investigations, even ones started promptly, take time to complete properly. This introduces delays in knowing data or knowing answers conclusively. It's very helpful for communications partners to know their client, and understand the way investigations will take place, as this can guide how they prepare their communications to key stakeholder groups. They will need to shape the right messages to help their client move forward seamlessly and avoid making unnecessary or detrimental statements.

You want to be prepared because silence is not going to help, particularly in a ransomware situation. Although it's a delicate balance because you don't want to be paralyzed by the fact that the investigation may take time to uncover definitive answers.

> You want to be prepared because silence is not going to help, particularly in a ransomware situation. Although it's a delicate balance because you don't want to be paralyzed by the fact that the investigation may take time to uncover definitive answers.

Manny: One thing we've seen in more recent ransomware incidents is a lot of transparency in large-scale ransomware incidents where the victim organization is detailing the steps they have taken or will take to address the incident, as well as identifying the environments that were impacted by it, to the extent that they can.

Mike: What is the most common pitfall you believe companies should guard against in remediating and recovering from a cyber incident? Is it jumping to conclusions too soon? Impatience to return to normal? Other things that you're seeing?

Manny: I'd say both of those things are true, but one that I see more often than not in these types of incidents is losing sight of what the goal or objective is during remediation. So, separating out what your long-term or strategic remediation goals might be, versus the steps that need to be taken for containment — in other words, focusing on what needs to be done to shut the incident down and ultimately ensure the attacker no longer has access.

Brice: One thing I'd like to add — and I run into this quite a bit when we conduct penetration testing for our clients — is assuming that your remediation is complete by only containing the immediate alert received. Some people assume that changing the password and isolating the server is enough to address a privileged account gaining access to a server and performing a malicious action. However, doing this may have only alerted the attacker that you're aware of them and ultimately achieved very little else.

Given the advanced techniques of today's adversaries, the attacker most likely has some other form of access into the environment, enabling them to continue their mission. This presents a false sense of security and containment.

Mike: Is it possible to achieve that level of certainty that you've achieved containment?

Brice: I think you're essentially looking at it as a degree of comfort, and that comfort is based on experience in seeing what attackers do, how they maintain access, what their objectives tend to be, etc. And that comfort grows over time, especially if you have visibility into how the attacker may try to get back into the environment, for example. That's always good evidence of successful remediation and containment — if the attacker is getting more desperate to regain the access they once had. But again, you're very much reliant on informed intuition.

Manny: For visibility, if you have a higher degree of visibility coming out of an incident, and you're able to see what the gaps were that allowed the incident to take place, you're going to have greater confidence that containment or remediation will be successful.

Mike: Cyber incidents often have both a technical and a human component. What's your perspective on how companies should best prepare ahead of time to manage on both fronts?

Brice: There's a business component to an incident, and that's usually best handled by conducting a solid tabletop exercise that works through key questions across the business, executive, and incident management teams. How will leadership be involved? How will you communicate to employees and customers? And to the extent you need to prepare for remediation, there are various internal moving parts regarding the investigation and response itself. Proactive assessment and preparation put an organization in a better place to figure out how to successfully remediate, contain and kick the attacker out.

Mike: You mentioned tabletop exercises. Are there other trainings or training courses that organizations maybe have overlooked or not prioritized that could be helpful?

Manny: Yes, certainly. The more training a security organization can receive, the better the organization will be. So, things like incident response training and courses that focus on the enterprise aspect of an incident, rather than a single system forensics or e-discovery, are going to speak to remediation and containment, but also managing an incident from a more holistic view.

Brice: IT system administrators are a major part of an organization's capability to defend against cyber adversaries. Exercises like red team training can give IT administrators good experience with how their environment can be misused or manipulated in a way that would enable an attacker to achieve their main objectives. This can only help an organization grow and mature.

There's a business component to an incident, and that's usually best handled by conducting a solid tabletop exercise that works through key questions across the business, executive, and incident management teams.

Brice (cont.): I've had a lot of good experience with what I'd like to call a collaborative red team assessment, which is sometimes referred to as a purple team assessment. It means having a security operations center, or a broader security team, work very constructively with the set of penetration testers that are conducting the assessment. This adds value because a lot of times we're making educated or informed decisions as consultants about what the attacker actually did that caused X or Y evidence to be there. We're piecing all of that together. But with penetration testers, security teams have an opportunity to make use of those professionals to understand what was done to exploit the system.

BRICE DANIELS
Director, Mandiant
Brice.Daniels@mandiant.com

MANNY JEAN-GEORGES
Manager, Mandiant
Emmanuel.Jean-Georges
@mandiant.com

PAUL HOLMES
Global Managing Partner,
Finsbury Glover Hering
Paul.Holmes@fgh.com

MIKE DOLAN
Managing Director,
Finsbury Glover Hering
Mike.Dolan@fgh.com

NEW YORK

+1 646 805 2000 | enquiries-us@fgh.com