BRP

CYBER CENTER OF EXCELLENCE

REVELATIONS, REGULATIONS, & RISKS

CYBER EXPERTS WEIGH IN

Part Two: Incident Response

INSGROUP

A BALDWIN RISK PARTNER

DAVID KRUSE

DIRECTOR OF INSURANCE ALLIANCES
ARCTIC WOLF INCIDENT RESPONSE

ARCTIC WOLF INCIDENT RESPONSE

David Kruse is the Director of Insurance Alliances at Arctic Wolf, the leader in security operations and incident response. At Arctic Wolf, David works with cyber insurance carriers and brokers to deliver services and tools that help businesses of all sizes and industries reduce the frequency and severity of cyber-attacks, and should one occur, respond to them with a full-service incident response program. Prior to his current role, David was the Cyber Practice Leader at Hausmann Group, an insurance and risk management firm based in Madison, WI, where he advised the firm’s clients on how to align their cybersecurity practices with cyber insurance requirements to achieve the best risk transfer results.

“A GOOD BACKUP THAT YOU CAN USE DURING A RANSOMWARE EVENT IS YOUR GET OUT OF JAIL FREE CARD.

WE ASKED, DAVID ANSWERED

Q: WHAT IS THE ROLE OF AN INCIDENT RESPONDER?

A cyber insurance policy provides the funds for recovery and the framework for the response effort itself. An incident responder plays a vital role in enabling investigation, remediation, and recovery within this framework. These services are often challenging to access without an insurance provider's assistance. Investigating the root cause, tracking down threat actors, negotiating ransom demands, and restoring systems require specialized expertise. The goal is to get you up and running as quickly as possible so you can get back to business. While the insurance policy aims to make you financially whole, the incident responder's job is to make you technically whole.

Q: WHAT KIND OF THREAT ACTORS ARE YOU MOST CONCERNED ABOUT RIGHT NOW?

Threat actors that specialize in data exfiltration (without corresponding data encryption) could be especially dangerous as more data privacy laws and regulations come into effect.

Threat actors continue to exploit encryption in their attacks, aiming to disrupt networks. Encryption is still very common, but as threat actors evolve, ransomware events are often data exfiltration/extortion events and may or may not include encryption.

An increasing number of companies are adopting EDR tools (Endpoint Detection and Response) to detect and respond to threats. These tools are instrumental in identifying threat actors before they can lock up a network. Having an EDR tool makes it more likely that you can thwart an encryption before it’s completed. In response to this, threat actors are changing tactics and opting to steal data for ransom, as seen in the MOVEit vulnerability. In this case, there was no encryption involved; instead, the focus was on data exfiltration. This trend, coupled with burgeoning data privacy laws and regulations, could spell trouble for compromised businesses.

Q: DID YOU SEE ANY PARTICULAR TYPE OF DATA BEING TARGETED?

Threat actors are good at a lot of things – what they're not particularly good at is determining what data, if lost, will have the biggest impact on a business.

For example, a threat actor might obtain a financial disclosure record to hold for ransom without realizing their target is a public company that is required to share the information anyway. This shows there's not always a lot of rhyme or reason for what they go after. In this case, they probably just went after whatever was available and played what they believed was their "strongest" card.

It's not atypical for them to go after expected things, like human resources records, internal financial records, or even a copy of the cyber insurance policy. Those tend to be regular targets in an event like this. It's harder for threat actors to understand third-party confidential records for a business deal, blueprints, or a business document set. If they can find personal information, like social security numbers or addresses, they're going to take that instead because they know that is going to be more sensitive data.

Q: WHAT IS YOUR BIGGEST CONCERN IN THE CYBER INSURANCE INDUSTRY?

We focus too much about the controls that are easy to talk about, leaving us the most vulnerable to the things that can hurt us. Take awareness training for example. I agree it’s a critical control, but I worry that we (carriers, brokers, security firms) sometimes ascribe too much weight to it to the detriment of other, more impactful controls. While we all know what it's like to take a short video and quiz for user awareness training, our own investigative incident response data reveals that these measures address only about 10% of ransomware cases. The broader causes of network intrusions aren't deterred by user awareness training.

The overwhelming cause is external exposure issues, like remote desk protocol open on public internet, not patching known software vulnerabilities, and having misconfigured VPNs. These technical risk controls have nothing to do with user awareness training.

So, what I worry about is that the industry focuses too much on controls that are easier to talk about (like awareness training) and not enough of controls that are more technical (and maybe more difficult to discuss) but more effective. External exposure monitoring and backups are the primary ways to prevent the frequency and severity of cyber incidents.

Q: SO, ARE YOU SAYING THAT EVERYONE IS POTENTIALLY A TARGET?

To understand why everyone is a target, it’s important to understand how threat actors identify targets. Step one is to identify a technical vulnerability they can exploit. Step two is to identify potential targets who have the technical vulnerability. This is often accomplished by using a website called Shodan.io or from buying access to the targets from other threat actors known as “initial access brokers’.

For example, if I know of a vulnerability that allows me to compromise a specific type of VPN, I'm going to use Shodan to find every VPN of that type. That’s going to give me a hit list of companies to start compromising. Only after I’ve done this will I check to see which companies I compromised. It might be a mega Fortune 500 firm, or it might be a mom-and-pop landscaper.

If it’s a targeted attack, like a spear phishing email attack, they might do some homework beforehand to identify specific targets, but in most cases, they don’t know what company they’ve hacked until after they’ve hacked them.

Find Out if You’re a Potential Target

Download Our Infographic Here

Q: WHAT MAKES YOU PANIC ON AN INITIAL SCOPING CALL?

It is our job not to panic, but there are absolutely moments when we see things that make us realize this is going to be a longer, or more involved, engagement.

During the initial scoping call, we learn a lot about the company, including details about the attack, suspected threat actors, initial information regarding the client's network, and the nature of their business. The client's knowledge of their own network plays a crucial role in our response effectiveness: the more they can point us towards where the fire is (and what might be on fire), the better we'll be as firefighters. Understanding your own network is vital. If you've done network and data mapping exercises, created an inventory of hardware and software assets, and defined roles and responsibilities, your case will go more smoothly. This proactive approach enhances attack prevention and response efficiency.

On a scoping call, we'll also get our first clues about whether a ransom payment may be needed. In cases where backups are encrypted or located on the network, paying the ransom for the encryption key may be the only option. We will always attempt other restoration methods, and paying is always the last resort; but companies should think about what it would take to make them pay a ransom, and then work backward to avoid that scenario.

The most important lesson for clients regarding ransomware is this: a good backup that you can use efficiently during a ransomware event is your 'Get Out of Jail Free Card'. It will have such a meaningful impact regarding how quickly you can get back up and running and what the total cost of that incident is going to be for you. Define a recovery time objective, and then resource that objective to ensure it's workable during an incident.

Q: WHAT DO YOU THINK THE HOTTEST TOPICS FOR INCIDENT RESPONSE ARE GOING TO BE FOR THE END OF THE YEAR?

I'm curious about the effectiveness of the feedback loop from incident response to claims to underwriting, brokers, and clients in response to the reality of the 2023 ransomware landscape.

2022 saw an artificially depressed ransomware environment because Russia invaded Ukraine, causing the biggest threat actor group to collapse. That group has disbanded, and their members have now joined many other groups. Now, the entire ransomware environment is even more robust. At the end of 2022, we saw rates start to level out, even dip in some cases. I’m curious how carriers are going to adjust these rates to account for the massive ransomware increases we’ve seen this year.

On the incident response side, we want to provide anonymized loss information back to the insurance community because to enable them to help prevent these attacks, we need to share how these attacks occur. I’m curious to see which carrier and broker markets are most willing to take in and use that information, and how it impacts their decisions for the beginning of the year and beyond.

Q: WHAT ARE SOME THINGS THAT CLIENTS CAN DO WHEN THEY HAVE A SUSPECTED INCIDENT?

One thing that we've seen more of in the past twelve months than ever before is claims coming to us from insurance companies for pre-ransomware. This is great because it shows that companies have tooling in place to identify these events before they happen and that they are also aware of the need to notify their carrier and implement incident response.

From a technical perspective, detecting the ransomware kill chain from the initial system compromise and having a human to act is an enormous advantage. Once encryption occurs, your options are limited to backups or the threat actor's mercy (good luck with that…).

A pre-ransomware state is a race against time. Threat actors recognize when they're being watched and they're going to start to rush. As soon as you notice those indicators of compromise, file that claim before you take your next breath. Get an incident response firm in there because you might be able to thwart a major event coming down the pipe. That's as much a technical action as it is a process action.

Make your IT team aware of your cyber insurance policy and even discuss giving them the authority to file a claim. Ensure they also alert whoever purchased the policy, as they need to be involved, too. We'll hop on a scoping call and give you a pulse check. If nothing comes of that call, it won't affect your claims history and you won't be billed. It's better to have us check it out and end up being nothing than let a threat slip through the cracks.

Q: SO, WHAT YOU’RE SAYING IS WORK WITH A BROKER THAT REALLY UNDERSTANDS THE INS AND OUTS OF THE POLICY, INFORMS YOU ABOUT THAT PRIOR TO AN EVENT, AND ALSO HAS CONTACT WITH YOUR IT TEAM?

That’s exactly what I’m saying! Insurance brokers are in such a powerful position to help ensure the client has the best risk transfer mechanism in place, but also to recommend steps to prevent a cyber event. A great broker can help you understand how to utilize the services the policy offers to inject an incident response team that will help prevent an encryption event from happening.

SEE OUR KEY TAKEAWAYS:

Collaboration is critical to mitigating cyber exposure. Evolving cyber risk requires companies to coordinate preventive measures companywide, utilize the best security controls, and work closely with trusted partners in the cyber security community.

The BRP Cyber Center of Excellence provides more than expertise in placing cyber insurance coverage. We offer a broad range of integrated solutions and services that provide value to our customers by limiting the potential financial and operational impacts of cyber incidents. We work closely with companies across every industry to identify their specific vulnerabilities, mitigate current cyber risks, and stay ahead of new risks emerging on the horizon.

BRP
CYBER CENTER OF EXCELLENCE

INSGROUP
A BALDWIN RISK PARTNER

CONTACT US TO HELP PROTECT YOU AND YOUR BUSINESS.

BRP

CYBER CENTER OF EXCELLENCE

INSGROUP

A BALDWIN RISK PARTNER

This document is intended for general information purposes only and should not be construed as advice or opinions on any specific facts or circumstances. The content of this document is made available on an "as is" basis, without warranty of any kind. Baldwin Risk Partners, LLC ("BRP"), its affiliates, and subsidiaries do not guarantee that this information is, or can be relied on for, compliance with any law or regulation, assurance against preventable losses, or freedom from legal liability. This publication is not intended to be legal, underwriting, or any other type of professional advice. BRP does not guarantee any particular outcome and makes no commitment to update any information herein or remove any items that are no longer accurate or complete. Furthermore, BRP does not assume any liability to any person or organization for loss or damage caused by or resulting from any reliance placed on that content. Persons requiring advice should always consult an independent adviser.

Baldwin Risk Partners, LLC offers insurance services through one or more of its insurance licensed entities, including but not limited to Insgroup. Each of the entities may be known by one or more of the logos displayed; all insurance commerce is only conducted through BRP insurance licensed entities. This material is not an offer to sell insurance.