semperis

How Staffing Reductions Increase Ransomware Risk

Semperis CISO Jim Doggett on Holiday Staffing Gaps and Ransomware Recovery

ISMG

Ransomware actors exploit predictable staffing gaps during weekends and holidays. Reduced coverage creates delays in detection and response, giving attackers time to escalate access and lock critical systems, said Jim Doggett, CISO at Semperis.

Findings from Semperis' 2025 Ransomware Holiday Risk Report, based on a survey of nearly 1,000 organizations, showed a slight decline in ransomware frequency compared with the prior year. Timing, however, played a decisive role. Roughly 60% of attacks occurred on weekends or holidays, when many organizations reduced security staffing by close to 50%.

"If a bad guy wants to get in bad enough, he will get in," Doggett said. "You have got to assume that you are going to be attacked and they're going to successfully get in."

He said most organizations invest heavily in prevention and detection but struggle with response execution. Identity platforms-such as Active Directory and Entra ID remain central targets because outages halt authentication, access and application usage across the enterprise.

In this video interview with Information Security Media Group, Doggett also discussed:

- Why mergers and acquisitions create new ransomware entry points;
- The risks of reduced weekend SOC staffing models;
- How repeated recovery testing shortens outage duration.

Jim Doggett

CISO, Semperis

Doggett leads Semperis' cybersecurity strategy, managing its security posture, risk management and resilience programs to protect identity systems and defend against cyberthreats. A veteran with more than 35 years of experience, he drives risk-based security and operational resilience.

HOLIDAY RISK REPORT PURPOSE

TONY MORBIN: What's the need for a holiday risk report, and who's the audience for this report?

JAMES DOGGETT: Typically, we do things that are for a CISO, but in this case, it's also probably for boards of directors and some of the senior management. And the reason is we had several questions that we were trying to resolve. Where's the world of ransomware going? Is it increasing? Is it decreasing? What are the characteristics? We interviewed nearly a thousand different companies and got their take on what's going on in the world of ransomware, with the hope of learning some things that can help us do a better job of addressing it going forward, or maybe understanding if it is going away.

"We know now that weekends and holidays are an attack vector. And on top of that, we're finding out that people don't staff as much, which makes it much harder to react and even detect that attacks are happening."

UNDERSTANDING RANSOMWARE ATTACK PATTERNS

MORBIN: Was there anything in particular about ransomware that you were hoping to get from the report?

DOGGETT: There were three or four things we were hoping to get. Number one is frequency. Is the frequency of people being attacked increasing or decreasing, which is sort of interesting because we did find there was a slight decrease this year over prior years, which is fairly interesting. Other things that we were seeking included understanding whether there is a time element to when ransomware attacks occur or do they occur randomly or do they tend to focus on weekends and holidays. It's things like that that we're trying to understand. We also wanted to get a better understanding of how people were getting in. Typically, when ransomware occurs, it starts with a fairly low-level attack, such as phishing, and then they escalate privilege to the point where they can deploy ransomware. They never directly attack the things that allow you to deploy ransomware. It always happens at a much lower base and it goes up. We were seeking information like that.

"Make sure you've dealt with the basics before you try to get the new shiny objects that are out there. And I will even include artificial intelligence as one of those today. It does no good to put all these controls around AI if you still aren't patching your systems or you are giving everybody too much access."

HOLIDAY RISK REPORT FINDINGS

MORBIN: Beyond the decrease in attack frequency, what other significant findings emerged? Were there any surprises?

DOGGETT: Several things that came out of that surprised me. Number one is we found that weekends and holidays saw a significantly higher occurrence of ransomware, and about 60% of all attacks from the people we interviewed occurred during weekends and holidays. There's some logic to that. You have to step back for a minute and think about, why would they attack on the weekend? Typically, people don't work on weekends. And it's sort of interesting that we did follow up and ask questions about how are you staffed?

If you have a SOC or if you have an external SOC that you've hired someone and outsourced it to, what do you do in terms of staffing on weekends and holidays? And we found it very interesting that people are trying to be nice to their employees so they don't want them to work as much on weekends and holidays, which means that they're not staffing.

On average, the companies that lowered staffing, lowered it by almost 50%. That surprised me. We know now that weekends and holidays are an attack vector. On top of that, we're finding out that people don't staff as much, which makes it much harder to react and even detect that attacks are happening.

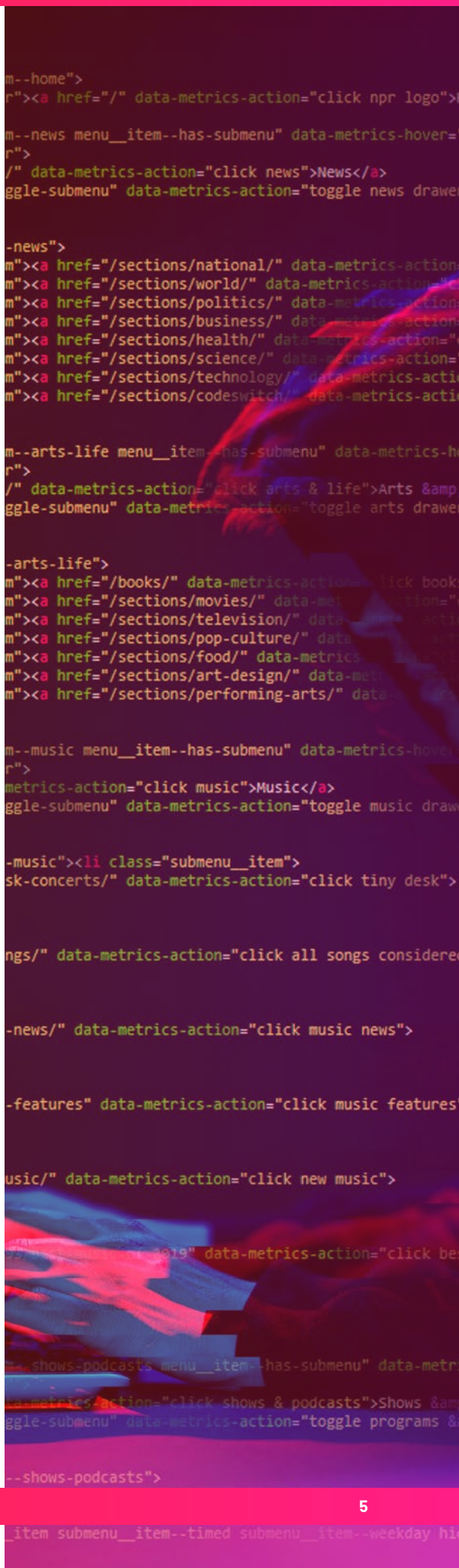
One of the recommendations people have to think very hard about is the need to increase staff over the weekends, which can even include choosing to do a hybrid approach - maybe of internal staffing on weekends combined with outsourcing. That should be decided by each company, but it's certainly something that needs to be addressed at this point.

ATTACK TIMING AND METHODS

MORBIN: Tell me about the types of attacks that were identified. Beyond the weekend and holiday pattern, was there a specific time-of-day pattern too?

DOGGETT: Typically, what they like to do is attack later in the evenings after 5:00 PM local time because people tend to go home and you don't fully staff. It's common sense, but we did prove it out in the study. That's another interesting thing that came up, which we didn't directly ask about at first, but it started to come out more and more: Attacks tended to occur very frequently when companies were going through mergers or acquisitions or some kind of big corporate event. Again, if you step back, that makes some sense, at least to me. If you're going through a merger, you're distracted and you're focused on other things. Also, typically when you have a merger or acquisition, security at one of the two companies is not on par with the other one. And if it's not on par, there might be a weak spot. You join those networks together, and guess what? You have got an easier vector to come in and attack.

That's another aspect. As far as how they're attacking, it's the same thing. I've been in this business almost 40 years now. It's the same thing as always. Probably some new stuff too, but it's still common phishing, all those types of campaigns—it always starts low level and then escalates. Also, it's a result of people not patching their systems and providing too much access. It's the same thing that we've been dealing with forever. And that's one thing that I tend to emphasize when I talk to CISOs: Make sure you've dealt with the basics before you try to get the new shiny objects that are out there. And I will even include artificial intelligence as one of those today. It does no good to put all these controls around AI if you still aren't patching your systems or you are giving everybody too much access.



IN-HOUSE SOC RISKS

MORBIN: What's the risk of keeping the SOC in-house?

DOGGETT: There are a couple of things. Large companies tend to have more in-house SOCs. You go to smaller companies, they can't afford to staff full time and have all the people you need to follow the kill chain. They tend to outsource a bit more. But that one risk of in-house is weekend staffing. If you're going to run at 50% staffing, that's probably not going to cut it if you're staffed in-house. Also, there's the challenge of getting the skills today to do it. That is difficult to do, especially if you're a smaller company. Then outsourcing might be better.

But if you choose to go the outsource route, the one thing I've always recommended is that you have to keep the management of that in-house. In other words, you don't outsource the whole thing and hope they do a good job. They're not your company, so they don't have the same vested interest. They don't own stock. I always highly recommend you have an internal personnel who takes that accountability to manage the outsourced team and be ready if your internal team needs to jump in.

DETECTION VS. RESPONSE GAP

MORBIN: What's your view on the opinion that there's too much emphasis on detection rather than response?

DOGGETT: First of all, when I say detection, I think of two things: preventing something from happening and detecting it either before or while it's happening. In today's world, there's too much emphasis on it because one thing I have learned through all my years is that if a bad guy wants to get in bad enough, they will get in. It's just a reality. Unless you want to unplug, there is no absolute. You have to address it by saying, "I've got to also assume that I'm going to be attacked and they're going to successfully get in. Now what do I do?" And that to me is probably is the biggest gap that CISOs struggle with globally. CISOs are good at preventing and detecting. They are not nearly as good historically at what we do when it happens.

In other words, incident response, crisis management, business continuity—how do we get back up and minimize the damage that's being done? That's hard. It's not a technical thing. It's a process thing. It's a people thing. Legal has to get involved. Communications has to get involved. I could go on and on, but that is a massive gap right now in most companies, large and small across the world, that need to step back and say, "CISO, you're now not only accountable for preventing and detecting, but also for how you respond." Ransomware is the perfect example. Prior to ransomware, CISOs didn't get blamed. They may have got blamed, but they weren't responsible for most of the big outages. They were fires and floods and things like that. Ransomware is right in our spot of security. We have to be ready, and they're going to come to us and say, "You're responsible. What are you going to do?"

BUILDING ORGANIZATIONAL RESILIENCE

MORBIN: What should organizations be doing now to bolster their resilience?

DOGGETT: There's a handful of things that I would recommend. Number one is they have to have a plan. Have they even thought about it? Have they stepped back and said, "Well, if this goes down, can I recover?" For most companies, this is the example that I always go in with and I say, "Okay, so you guys are ready. Your entire network's down and out. What are you going to do?" They say, "We'll copy it from backup and we'll get it right back up and running." And I say, "Well, how long will that take?" And then they start having some difficulty talking about how long it may be. And I say, "Have you tested that? Do you know if you can get back in that amount of time?" Then I go to the next question. I ask, "Have you thought about all the infrastructure that supports that?"

And this is where I would get into what we do for a living, which is Active Directory, Entra ID, in that space—if those things are out, how long will it take for you to recover those? And virtually no company or very few companies can answer that question because it is very difficult to test recovery of AD. It's not a copy and do it. It has to be installed and propagated throughout all your domain controllers. It's a fairly complex process, and typically, it takes multiples of whatever their RTO is. They need to get back in 24 hours. It may take weeks because you can't do anything if your infrastructure is down. You can't run an application if your infrastructure is down. You can't log onto the network to do anything if things are down. So that is a big area that everyone needs to start to focus on.

The second thing that I would also say is once you have that plan in place, you got to test it. Test it, test it again and then test it again. You don't build muscle memory by thinking about it and not doing it. You have to actually do it. And with a lot of these things, especially the infrastructure, you will find out all kinds of things you didn't know about that get in the way of doing a quick recovery. Because in the end, what you're trying to do is limit the damage. And if you haven't practiced doing that, doing it for the first time in an emergency situation where people may have slightly different roles can be really daunting.

THE SEMPERIS APPROACH

MORBIN: How is Semperis helping its customers prepare for ransomware risk, and where should our audience go to learn more?

DOGGETT: We're over a thousand customers now and typically we focus on the identity space. In other words, your identity store, what holds all your credentials, which when you think about it, is the key to the kingdom. Almost every application every company uses is dependent on that identity store being available to authenticate who the person is and what access they should have. If that's down, nothing works. You can't even log in to get your email. So that is an area that we have chosen to focus on. And again, I joined Semperis for that very reason. I came from a very large insurance company where we had an outage

of AD, and it was not an attack. It was a fat-fingering by an individual who made a mistake and knocked out roughly 20,000 users.

We went to backup. Of course, backup didn't work because we had never tested it. We didn't know how to install it anyway. We ended up hiring consultants for a month, expended roughly millions of dollars, lots of downtime and we recovered. So that's why I joined, because this is an area that people need to focus on at a minimum. Because when bad guys attack, they almost invariably —probably 90% of the time—go after your identity store, whether it is AD, Entra ID, Okta or whatever people are using.

We focus on that space and we approach it in three ways. We follow the MITRE ATT&CK framework. We look at it before an attack, during an attack and with that assumption that if you have already been attacked successfully, how do you recover quickly and minimize the damage? That's what we do.

You can visit our website at www.semperis.com to learn more and contact us.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of its 38 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, OT security, AI and fraud. Its annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(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 TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

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