Picture credit: AdobeStock

UNDERSTAFFED AND UNPREPARED:

Dan Lattimer *reveals how ransomware gangs are exploiting downtime and material corporate events*

Cyber criminals don't observe business hours – they create the perfect moment to strike when they know the Security Operations Centre (SOC) will be least prepared. While 96 percent of organisations run a SOC 24/7 for 365 days a year, 85 percent of these admit they reduce SOC staffing by up to 50 percent during holidays and weekends, according to Semperis' Ransomware Holiday Risk Report. What's more, in the survey of 900 IT and security professionals across the US, UK, France and Germany, 5 percent said they leave their SOC completely unstaffed during these times as opposed to using shifts or a follow-the-sun strategy.

Hackers have been quick to catch on to this pattern. They know that when they attack on holidays and weekends, companies are less prepared to respond. Some organised gangs operating like legitimate businesses even hire staff specifically to carry out attacks during these periods when organisations are most vulnerable. It is not surprising then that 72 percent of businesses reported they have been attacked over a holiday or weekend, with 86 percent suffering a ransomware attack. And, with fewer people manning the SOC, detection and response is slower, buying the attacker more time to encrypt and/or exfiltrate data.

76 percent of respondents experienced attacks during major corporate events when businesses are often under increased pressure

The question is: given this is now a known trend, why aren't SOC staffing levels being maintained more consistently? According to the survey, a third of organisations choose to scale back because they do not think it necessary to retain a full team outside of the five-day working week. The same number (34 percent) assume their organisation won't be targeted, while 33 percent consider such measures overkill given that their business hasn't previously been attacked.

Cost is also a consideration, with organisations keen to make cuts or avoid paying higher rates during evenings, weekends and national holidays. However, such penny-pinching seems counterproductive given that ransomware demands can stretch into the millions, with the average cost of a breach now standing at $4.88-million.

And it's not just holidays and weekends that leave organisations wide open to ransomware attacks. Material corporate events, such as mergers and acquisitions (M&A), IPOs, earnings releases, layoffs or a change in leadership are frequently targeted periods, too. In fact, the report revealed that 76 percent of respondents had experienced attacks during major corporate events when businesses are often under increased pressure.

Mergers can be a particularly vulnerable time, as any business going through the process will want to keep the deal on track, which means that cyber diligence can often be sidelined in favour of financial and operational expediency. It becomes much more difficult to maintain best practice during such events due to the level of disruption involved.

The restructuring that follows M&A deals can also create the perfect environment for attackers to go undetected for longer periods. Transition teams are often reluctant to disturb legacy systems, for instance. When patching isn't conducted on these systems or older, outdated software is no longer supported by the provider, they are inherently less secure, making them ideal targets.

In addition, post-deal, systems and personnel need to be integrated – which can see security compromised if one of the companies previously had a weaker security posture. This can act as a springboard for the threat actor, allowing them to bounce across into the more secure environment by compromising core, business-critical identity systems – such as Microsoft's Active Directory (AD).

AD is the most commonly used identity system for authentication and authorisation in on-premise environments today, while Entra ID or Okta are commonly used for identity management in the cloud. These systems are frequently the target of cyber criminals as they hold the keys to other services and applications across the company network. AD is compromised in 90 percent of ransomware attacks. And, if an attacker is successful in compromising AD, they can then escalate their access to the most privileged accounts to reach the most sensitive data.

In the event of an attack, it's therefore imperative that an organisation has the processes in place to rapidly recover its identity systems and restore access to key IT services. However, while 70 percent of businesses claim to have an identity recovery plan, a fifth admitted that the plan did not take cyber use cases into consideration, instead focusing on other scenarios such as outages or disasters. Moreover, 17 percent do not include measures to test for identity-specific vulnerabilities. The majority (61 percent) also do not have dedicated AD backup systems to ensure the system can be brought back online free from malicious software.

This is worrying as the ability to recover identity systems is a major part of being able to withstand and bounce back from a ransomware attack. It's going to become an even more pressing challenge as threat actors increasingly harness Artificial Intelligence (AI). In The near-term impact of AI on the cyber threat, the National Cyber Security Centre (NCSC) has previously warned that AI technology will make it easier for unskilled threat actors to gather information on access and target victims with more precision using GenAI-as-a-Service alongside Ransomware-as-a-Service. The same report offers some hope, however, stating that most ransomware incidents exploit poor cyber hygiene – such as ineffective management of identity access management systems – rather than using sophisticated attack techniques, making these attacks preventable.

THE MARRIOTT HOTEL GROUP INHERITED A BREACH WHICH COST IT £18.4-MILLION

So how can organisations be better prepared for out-of-hours ransomware attacks? Critically, this needs to be led from the top, with the C-suite prioritising ransomware defence and identity threat detection and response (ITDR). Every board should be viewing cyber security as a business risk rather than just a technological concern. If core systems such as central identity services are lost, the repercussions can cripple a business, leading to loss of revenue and reputational damage as well as the prospect of punitive fines for failing to meet compliance obligations. It is, therefore, necessary for the board to be appraised of the company's risk profile and to understand which systems are business critical and liable to impact operations.

When it comes to the SOC, it may not always be possible to run a full team, but the real test is how quickly that team can mobilise when a high-priority incident occurs. It's here where operational resilience comes in. If the business has effectively planned for and tested its ability to respond to such events, it should have sufficient people, processes and technology in place to deal with the incident. The response plan should be optimised to cover the most vulnerable high-risk areas.

It's also possible to fill the gaps created by lower staffing levels by using technology effectively. Automation can provide the necessary assistance in the SOC, helping to reduce the need for human monitoring and intervention. Once the attackers are in, they will need to escalate the attack and this activity will require them to make changes to previously static settings, thereby triggering monitoring systems. When it comes to AD, for instance, automated auditing and alerting, attack pattern detection, rollback or suspension of unusual changes can all be carried out automatically using ITDR solutions. Recovery, too, can

be automated provided that the business has a tried and tested identity recovery plan and a dedicated backup for AD.

But what about those instances where operations are disrupted due to corporate events? The FBI warned back in 2021 that M&A presents attackers with a prime target as they are able to destabilise these deals by threatening to go public after compromising either party. Yet only 10 percent of mergers consider cyber security as part of the necessary due diligence required prior to inking a deal, potentially resulting in critical risks missed.

PREPARATION FOR OUT-OF-HOURS RANSOMWARE ATTACKS NEEDS TO BE LED FROM THE TOP

There are plenty of examples where this has happened. An acquisition by Paypal in 2017 of TIO resulted in the payment company suspending TIO operations after it discovered a security vulnerability that exposed the personally identifiable information (PII) of 1.6-million customers. In another instance, the Marriott hotel group unknowingly inherited a breach when it acquired Starwood Hotels & Resorts Worldwide in 2016, exposing the PII of 500-million people. Marriott was subsequently fined £18.4-million, which was reduced from £99-million due to the company being able to argue it had put in place mitigation measures after the fact.

These examples serve as a warning on the importance of cyber security prior to as well as after a deal has been struck. Ideally, both organisations should audit one another's systems to identify potential vulnerabilities beforehand and certainly prior to any system integration. This makes sense not just from a risk mitigation point of view, but also financially as any cost to remediate issues should be factored into the deal. AD can be a good barometer of cyber health here as if it is not locked down, the chances are there will be other issues in the estate.

Post-merger, Change Management is a key factor in ensuring a smooth transition for employees, stakeholders and operations. However, if it's not done correctly it can result in disgruntled or former employees who pose a threat to the business. They might seek to get even by selling access information and credentials, making it essential that procedures are in place to revoke access.

In summary, while it's not always possible for SOC staffing to be maintained, this needn't result in lowered defences. During holidays and weekends, there will be less personnel, but that doesn't have to equate to an increase in exposure. Similarly, landmark corporate events should not see cyber security sidelined, but become part of the criteria used to evaluate the state of the business and ensure a smooth transition.

The fact that ransomware attacks are coinciding with these calendar events is undisputed. The attack against Transport for London, for example, occurred on a Sunday while the Colonial Pipeline attack in the US coincided with Mothering Sunday. But knowing this is happening should be a wake-up call to businesses to bolster their defences and boost their resilience. By making cyber security a business priority, ensuring the incident response plan is fit for purpose and tested more than once a quarter, and focusing on automation to fill the gaps created by a drop in the workforce, the organisation can mitigate the risk of falling foul of ransomware gangs ●

Dan Lattimer has over 14 years' experience in cyber security and is Area VP of the UK and Ireland at Semperis where he is responsible for growing sales and expanding its channel reseller partner programme.

Microsoft's Active Directory is the most commonly used identity system for authentication and authorisation in on-premise environments today

Picture credit: Tippa Patt/Shutterstock