Picture credit: AdobeStock

SURVIVAL OF THE FITTEST

Dan Lattimer *reveals why, with ransomware able to strike at any time, resilience is your best defence*

Thanks to the advent of digital commerce, AI helpdesks and globalisation, many organisations can today legitimately claim to be open 24/7. Unfortunately, cybersecurity hasn't always kept up with this changing operational tempo. As corporate cautionary tales continue to hit the headlines, cyber resilience is finally shooting up the boardroom agenda. But while it's easy for business leaders to demand, it's far harder to deliver. This is where a minimum viable company (MVC) approach can help.

Threat actors will always go after the lowest hanging fruit. That means hitting targets when they are likely to be least-well defended. It's not just the likes of M&S which can bear witness to this strategy. Boutique Australian insurance company Prosura was the most recent to fall, after a threat actor stole large quantities of data from the firm on New Year's Day.

Semperis research supports this hypothesis. Over half (52 percent) of global respondents who report being targeted by ransomware over the past year say the attack took place during a weekend or holiday. And an even larger share (60 percent) claim attacks took place after a "material corporate event" such as a merger or acquisition.

Over two thirds of UK organisations targeted by ransomware paid the ransom

This is another smart move from threat actors. Security teams may be unsure about their reporting lines and responsibilities during a period of tremendous upheaval like this. They may not even know whether their immediate future is with the company. They might also have been requested to work on pressing internal initiatives related to the merger/acquisition, distracting them further from their day job.

It doesn't help that many security operation centres (SOCs) are already under-staffed. According to one recent study around half (47 percent) of security professionals report that they or their colleagues are experiencing some level of burnout. More than one in ten claim they're close to leaving the profession altogether. Alert overload is fraying nerves and overwhelming teams. As threat actors continue to raise the stakes, the pressure on some becomes unbearable.

Against this backdrop, it's therefore not surprising that more than three-quarters (78 percent) of organisations cut SOC staffing by 50 percent or more at weekends and during holidays, according to the latest Semperis *Ransomware Holiday Risk Report*. The number one reason for doing so is to improve work/life balance for employees. But 6 percent do not staff the SOC at all outside of the regular working week. This would seem unnecessarily extreme, given how many attacks now fall on these days.

If it's this hard to staff the SOC, maybe more organisations should outsource to a 24/7/365 provider. Yet we found that things are actually moving in the other direction. Over three-quarters of respondents say they now run their SOC in house, a 28-percentage point annual increase.

While network defenders continue to struggle, as tech sprawl accumulates, their adversaries are going from strength to strength. Crypto payments to ransomware actors may have declined 35 percent annually in 2024. And the average payment may have slumped 66 percent between Q2 and Q3 2025. But there are still plenty of threat groups out there causing trouble. All organisations are potentially at risk. But there are those that realise this – and are actively taking steps to address security gaps – and those that don't.

If anything, changing market dynamics are forcing threat actors to innovate and adapt, as they have always done, in order to thrive. What we see is a blend of old and new. Yes, phishing, vulnerability exploitation and remote access compromise are still the top three methods of initial access. But increasingly identity is at the heart of these attacks.

This could either mean a simple spear-phishing email designed to steal corporate credentials or maybe a vishing attack either on the IT helpdesk (requesting a password reset), or impersonating IT. Misconfigured OAuth systems can further amplify the impact of attacks – enabling persistence and lateral movement across the app ecosystem. When no doors can be unlocked via vulnerability exploitation, there's always identity. With infostealers supplying the dark web with a steady stream of compromised credentials, there are ample opportunities.

Organisations can ill afford to be knocked offline by a serious cyber incident. Yet the data shows UK firms, at least, are not as resilient as they could be. In fact, over a quarter (28 percent) are categorised as 'at risk' – with average uptime across critical business services over the past 12 months just 73 percent, according to a recent report.

Semperis' research found that 58 percent of UK ransomware victims over the previous 12 months experienced data loss or compromise as a result of the attack. But even when data isn't lost, business disruption can be severe. Perhaps this explains why over two thirds of UK organisations who were targeted by ransomware paid the ransom – with 39 percent even paying multiple times.

ENTRA ID ADDS AN EXTRA LAYER OF COMPLEXITY TO THE PROCESS OF RESTORING ID SYSTEMS

On average, it took UK businesses over seven days to completely return their operations to a normal state. These extended business outages can create multiple business challenges. There could be a big bill for incident response and legal/professional services. And a potentially even larger one from lost sales.

The truth is that, even if data isn't encrypted, ransomware attacks can still end up taking their toll. Systems usually have to be taken offline, investigated, cleaned and then eventually restored – disrupting operations. And there's the added risk of data theft, which can impact the bottom line and reputation, via breach notifications, regulatory scrutiny, class-action lawsuits and customer churn.

Against the backdrop of an unforgiving threat landscape and a cyber-attack surface that expands with each new digital endpoint, CISOs are looking for new ways to enhance cyber resilience. A popular strategy involves defining a 'minimum viable company' (MVC). This is about stripping an organisation down to its essential infrastructure, services/apps and people: the bare minimum it needs to continue operating during a crisis.

Once CISOs have got boardroom buy in for the project, they need to speak to the business to understand what 'viable means' (eg: revenue preservation, customer obligations, regulatory requirements), and how long the MVC needs to operate for. The latter is key and will define a great deal of what happens next.

Then it's a question of mapping essential services/apps to business processes and infrastructure. Teams should understand where manual workarounds and alternative suppliers may be necessary and how cloud services can help. And they might think about how to draw defensive perimeters around their most critical systems in order to preserve business outcomes during attacks.

Tabletop exercises are a great way to work through this process. And once the MVC strategy has been defined, it should be continuously tested and iterated. The business and technology landscape is changing so fast that plans may soon become outdated. Remember: this is not a substitute for business continuity/disaster recovery (BC/DR) planning. While the latter is about continuity and recovery of important services over

time, MVC is about short-term enterprise survival. That said, it can be integrated into broader resilience and BC/DR efforts.

Of course, the MVC approach is not the only way to improve cyber resilience. There are many other ways to think about the subject. But all tend to agree that organisations cannot hope to reboot business operations during an incident unless they get their identity systems up and running. Put simply, if Active Directory and/or Entra ID is not restored, employees won't be able to log in to their ERP, CRM or other business-critical apps.

ORGANISATIONS CAN ILL AFFORD TO BE KNOCKED OFFLINE BY A SERIOUS CYBER INCIDENT

It's therefore somewhat reassuring that 90 percent of the organisations we polled last year say that they have an identity threat detection and response (ITDR) strategy. And nearly all of these companies have processes in place to scan for identity system vulnerabilities. But there's plenty of work still to do. Less than half have policies in place to remediate these vulnerabilities. Worse still, far from all of them (66 percent) include AD in their disaster recovery planning or feature automated system recovery – which is crucial for resilience. It's not just speed that's important. So is ensuring that backdoors and compromised accounts aren't reintroduced when systems are restored. Identity forensics and incident response (IFIR) can help here. These tools are able to malware-proof backups by decoupling AD from the underlying OS. They can automatically clean up metadata, rebuild the Global Catalog and restructure site topology, among other things.

Entra ID adds an extra layer of complexity to the process of restoring identity systems because it creates new entry points for attackers, changes the permissions model (as identities are stored in the cloud) and makes visibility more challenging. IT teams are best off choosing tools that give them a single view of the hybrid identity environment and the ability to spot attacks and automate rollback centrally.

It's also worth remembering that threat actors don't usually attack AD directly. They're more likely to move laterally, exploiting vulnerabilities and misconfigurations in order to discover potential attack paths. Organisations can reduce their workload from a defensive/resilience perspective by focusing only on those assets closest to Tier 0 infrastructure. In this way, they can identify the most important attack pathways. Then it's decision time: either add these assets to Tier 0, close down the pathways or monitor them carefully.

The bottom line is that ransomware can eat into profits, disrupt operations and ramp up reputational and compliance risk. CISOs have a duty to ensure that their board knows what's at stake. And with an MVC plan, they can offer a pragmatic way to keep the lights on, in a worst-case scenario ●

Daniel Lattimer, Area Vice President, Semperis brings over 14 years' experience in the security market. His main focus is on operational resilience and working with organisations to better protect Active Directory.

Marks and Spencer lost around £300-million to a cyber attack in 2025

Picture credit: GianniM