Chartered Institute of Information Security

Pulse:

November 2022

CIISEC LIVE 2022

We finally made it to the Craiglockhart Campus in Edinburgh

CIISEC INNOVATION SUMMIT 2022

Themes included Cloud, Supplier Management, Human Behaviours

RANSOMWARE

The subject that cyber professionals can't seem to get away from

HOW TO BUILD CYBER RESILIENCE AS YOU ADOPT SAAS AND CLOUD TECHNOLOGIES

Tal Mozes
Mitiga CEO and Co-Founder

Over the course of the COVID-19 pandemic, many organisations adopted cloud services, particularly Software as a Service (SaaS) solutions. Slack and Zoom emerged as vital connectivity channels, while security teams familiar with on-premises solutions suddenly needed new skills to handle changing risks as they increasingly adopted SaaS and cloud solutions.

SaaS introduced many solutions into organisations, often without oversight from the security team. The new mesh of solutions is difficult to control and manage, and visibility for detection and response purposes is even more challenging. As the multi-year pandemic continues, it has become clear to security professionals that the cloud was not simply another endpoint hosted by someone else but a new set of technologies with different requirements and capabilities.

New technologies, new approaches

While delivering on scalability and availability, SaaS and cloud technologies also change how organisations need to approach incident response. The days when incident response meant boots on the ground, unplugging machines, and disconnecting from the network are over. But the days of cyberattacks and critical incident response are not. SaaS and cloud adoption requires an innovative approach to incident response (IR), one that can be delivered rapidly and at scale.

To respond effectively to critical incidents today, security teams must understand:

- SaaS platforms are owned by third parties, so we have less security control, making it harder to investigate during a breach.
- Investigators now often rely on third-party cooperation to access forensic data needed for an investigation.
- Cloud Service Providers (CSPs) operate on a shared responsibility model — and we need to understand where that begins and ends.
- The shared responsibility model means we may not have access to all the forensic data needed for an investigation, nor the time available to acquire it.
- There are different limitations on how we investigate SaaS and cloud incidents, and we need to understand how to compensate for those limitations.

We are no longer measured only by our ability to identify, protect, and detect serious cyberattacks, but also by our ability to respond and recover from those critical incidents.

> The days when incident response meant boots on the ground, unplugging machines, and disconnecting from the network are over.

Operational resilience requires cyber resilience

Operational resilience is both a best practice and requirement for organisations; cyber resilience itself is a subset of overall operational resilience. Today, security leaders are measured in terms of resilience: how fast we can return to business as usual. To do that, we need to invest in both proactive solutions and proactive approaches.

We can accelerate incident response by adopting automation, collecting and storing forensic data before we know an incident has occurred, and sharing knowledge across different organisations. We can also increase our readiness (or cyber resilience) to attacks by regularly reviewing, testing, and improving our incident response plans and capabilities. This increased readiness, coupled with the data needed for an investigation, can help incident responders begin investigating a breach within minutes, not days, and return to business as usual more rapidly.

MITIGA