CYGNVS

The First 48 Hours:
Why Cyber-Attack Response Plans Go Awry

The First 48 Hours: Why Cyber-Attack Response Plans Go Awry

Even the most sophisticated incident response plans often fail in their hour of need, and organizational challenges are at the heart of the problem. This paper explores where they go wrong and how to enable a laser-focused response when—not if—a cyber-attack strikes.

The best laid plans

Cyber risk best practices start with having a robust Incident Response (IR) plan in place. A first step is to map out the who, what, and when of those crucial first 48 hours so when an attack strikes the organization has the upper hand. At that early stage, a fast and efficient response is vital: the hours and even minutes saved limit the economic and reputational damage.

But what if the real-life event does not play out as expected? What if you have detailed and rehearsed plans in place covering everything from a fast system restoration to satisfying regulatory demands, but an unforeseen twist in events derails those critical first few hours?

This is a common occurrence. Problems we regularly witness include hackers infiltrating emails so organizations cannot securely unroll their IR plans; panic leading to poor decision making; absent or remote employees slowing or even harming the rehearsed response; and IR plans that are overly dependent on one key individual who could be unwell or – as we see too often – turn out to be the attacker itself.

While there are many reasons why IR plans do not always go as intended, there is one common thread: the weak points often stem from organizational challenges rather than IT challenges. More specifically, they stem from an inability to control and coordinate the performance of individuals in a crisis – a form of people risk.

Our experience shows that even the most sophisticated cyber IR plans typically overlook people risk. A threat actor's game plan is to hunt down any vulnerability and expose it: not just IT vulnerabilities, but organizational ones too. If people risk is your blind spot, they will find it.

The top three vulnerabilities

Where do the biggest challenges lie? According to the CYGNVS cyber team, which has decades of experience working with organizations during cyber attacks, there are three common weak points when responding to an attack.

First, communication. When an attack strikes, it is vital that those coordinating the response give fast, clear, and regular direction to their organization and relevant third parties. The speed of response is especially important. Waiting half a day to coordinate a global conference call is a common mistake: minutes and hours matter.

A typical first hurdle in many attacks is finding that the organization's email and other communication channels are compromised, leaving them with no secure means of communicating. This delays the response, often by days.

CYGNVS enables a laser-focused response when—not if — a cyber attack strikes.

Many companies are forced to resort to using personal messenger accounts. Not only does it take time to gather all employee details and create relevant groups, but companies quickly encounter problems. Not all employees will use the same personal apps, and furthermore, personal accounts pose security risks and often have limited functionality.

Even if the usual channels remain secure, they may not be centralized, leading to siloed or chaotic reporting lines that are hard to monitor or control.

Second, the reality gap. From the second a cyber threat is suspected, a detailed chain of actions is triggered, from closing down the cyber threat as fast as possible to notifying the company's insurers and regulators. The chain of actions is complex and multifaceted, involving many different teams and external stakeholders, often globally.

Experience shows that even the most rehearsed plans are often hampered by real-life realities, creating a "reality gap." Fluid team rosters and key employees working remotely are commonly reported challenges. Meanwhile, in a crisis, decision making can be impaired and rehearsed plans are forgotten.

According to the Ebbinghaus Forgetting Curve, humans forget approximately 70% of what they learned after just one day.[1] IR plans are, therefore, easily undermined by employees failing to follow basic training.

How our brain changes in a crisis

A common mistake in crisis planning is underestimating the impact a crisis has on how our brain functions and our ability to make effective decisions. Research reveals that, under intense stress and possible information overload, we tend to miss the nuances of even the most basic messages.

Common examples include:

- Not fully hearing information because of our inability to juggle multiple facts during a crisis
- Not remembering as much of the information as we normally could
- Misinterpreting confusing action messages.

As a result, many of us bypass a logical and reasoned approach to decision making. Instead, we may rely on habits and long-held practices, or we might follow bad examples set by others. Without the tools in place to counter these instinctive tenden-cies, our ability to respond effectively in a crisis is impaired.

The good news is you can take steps before a crisis that compensate for the changes our brains experience during the crisis. For example, having established communica-tion channels and a rehearsed crisis plan makes it harder for crisis-related stress to crowd out rational thinking.

1 Brain Science: The Forgetting Curve–the Dirty Secret of Corporate Training; learningsolutionsmag.com

Third, documentation. In the heat of the moment, the last thing any crisis team wants to worry about is administrative duties. However, having a secure and clearly documented timeline of events is vital for limiting liability. Regulatory requirements, potential legal action and internal investigations may demand a timeline of events and forensic evidence.

The reality of a cyber crisis is often chaotic, making documentation a challenge. Team leaders are absorbed by the core priorities of restoring business-as-usual and minimizing the immediate damage. It is not until after the event that the need for appropriate documentation is realized – by which point it is too late.

Closing window of time

All of the above three challenges are intensified by the pressure of time. When an attack occurs, the speed of response in the first 48 hours can make the difference between a minor incident and a major crisis.

The time pressure comes from three sources:

- **First, minimizing the extent of the cyber attack.** The first 48 hours of an attack are typically when the criminal gains control of core systems and establishes the advantage. The faster the response, the smaller the damage. In one cyber attack last year, threat actors deployed ransomware in less than four hours after compromising the organization's systems.[2] Once ransomware is executed, company data can be encrypted within minutes.[3]
- **Second, reporting requirements.** Many sectors have regulatory requirements to report cyber incidents within a certain timeframe. Some companies may also have contractual obligations to notify third parties in their supply chain. If the crisis is under control by the deadlines, reputational damage is minimized.
- **Third, going public.** Companies that are consumer facing, publically listed or high profile may need to issue a public statement early on in the crisis. As with the reporting requirements, companies that have achieved a swift and efficient response will have greater control of the reputational consequences.

The reality of this time pressure is extraordinarily challenging. Indeed, this closing window of time only heightens the importance of effective communication, the smooth implementation of IR plans, and an efficient documentation system.

CYGNVS: support in a crisis

CYGNVS is the first of its kind: an all-in-one cyber risk preparation and incident management platform. Its goal is clear: to help businesses prepare for the day they experience a cyber incident. Its secure, out-of-band environment is designed precisely for when disaster strikes, providing encrypted communication channels, centralized file storage, step-by-step frameworks for managing a cyber incident, and much more.

2 4-Hour Time-to-Ransom Seen in Quantum Attack as Accelerated Ransomware Increasingly Common | SecurityWeek.Com; April 2022
3 Ibid

Make employees your strength in a crisis

At CYGNVS, our aim is to make sure your business functions at its best in a cyber crisis. No surprises or blockages caused by overlooked people risks: the real event plays out like the rehearsed event. We want to get you back to business faster.

Based on our first-hand experience of managing real life cyber threats, the CYGNVS cyber incident response platform is designed to minimize the three core vulnerabilities described above. Its simple design gets entire businesses moving swiftly and in concert with each other in times of crisis.

Immediate, secure communication channels: CYGNVS provides a secure, out-of-band platform for communication. It is "always on" and ready for the moment a cyber threat is first suspected. Communication rooms are easily segmented by workstream, and permissions assigned to restrict users to specific rooms. For example, it is straightforward to include third parties such as lawyers and insurers, many of whom are already on the platform, and ensure they are only privy to conversations that are relevant.

No reality gap: CYGNVS ensures that IR plans roll out as intended by reducing room for human error. The platform helps break down plans into actionable tasks assigned to individuals. Everyone can see what needs to be done and by whom – including third parties and remote employees. Individuals get push notifications to keep them on track while team leaders can view progress. With key documents stored centrally on the platform, all employees have easy access to the same versions.

The cumulative effect of CYGNVS' capabilities is to minimize the people risk of a cyber attack. Indeed, evidence shows that using CYGNVS cuts the cost of a cyber attack by an average of 25% to 37%.[4]

With CYGNVS, the time and money invested in cyber talent and IR planning will shine through. It means that those crucial first 48 hours are not spent getting your house in order, but doing what is needed: restoring business as usual.

Leap frogging the maturity curve

Despite the highly publicized severity of cyber risk, cyber resilience remains immature for many companies. A large percentage have yet to find the resources to prioritize even basic incident response plans for cyber. This is especially the case for small and medium sized businesses (SMBs) that may not have a dedicated IT department.

The good news for these companies is that CYGNVS provides a fast track along the maturity curve. Research shows that downloading the CYGNVS app and onboarding your team will make a business more prepared than 65% of organizations[5] in terms of cyber readiness. It then provides a springboard to go further with access to best practice guides, templates, simulations, and desk-based exercises.

4 CYGNVS analysis, 2022
5 CYGNVS analysis, 2022

The First 48 Hours: Why Cyber-Attack Response Plans Go Awry

For those companies that are already in the top tier for cyber resilience, CYGNVS provides the chance to strengthen and scale their cyber-attack readiness. For example, your company may have the most thorough and sophisticated IR plan, but will your colleagues in London, Johannesburg and Tokyo respond in concert in the event of an attack? Will the plan fall apart if certain key individuals are unavailable? How will employees respond if they haven't had their training yet?

There is a large but subtle gap between a prepared company and a company with prepared individuals. CYGNVS minimizes this gap by providing the tools to manage hundreds of individuals and coordinate global teams. It brings depth and consistency to even the best plans.

Be the best in a crisis

A fast and focused response to a cyber attack is critical to reduce the financial and reputational impact of the incident. Unfortunately, experience shows us that many organizations, large and small, struggle in those all-important first 48 hours.

Whether you are an SMB with limited resources to focus on cyber risk, or a large multinational with global offices to coordinate, executing cyber IR plans are fraught with challenges, many of which will not surface until the real event hits.

Despite the fact that all cyber events are unique, the underlying problems reported by those that have been through them are the same: poor communication, a failure to execute IR plans as intended, and a lack of documentation. All these problems relate to the challenges of managing people in a crisis. At CYGNVS, our goal is simple: to help businesses be their best in the moment a cyber attack happens. It enables all individuals, including third parties, to work in concert with each other via strong, centralized communication; clear direction to employees globally; and non-burdensome documentation.

Cyber resilience is about more than having a robust technical defense or IR plans ready to dust off: it is about being your best in a crisis, from the top of the organization to the bottom. Your people should be your strength during a cyber attack, not your weakness.

Serving over 1,500 clients around the world, the team of experts at CYGNVS has pooled together best practices from managing tens of thousands of incidents to build the leading Cyber Incident Command Center. The CYGNVS platform is designed for enterprise-grade security with SOC2 Type2 compliance, ISO 27001 certification, and 24/7 live technical support. Learn more about how CYGNVS can help your organization plan, practice, respond and report during a cyber crisis.

CYGNVS

WP1.3.1.24

US +1 650 684 2040 I EU/UK +44 20 8089 5851
INFO@CYGNVS.COM
4940 EL CAMINO, SUITE 100, LOS ALTOS, CA 94022