DXC TECHNOLOGY

How response teams can control emotions during high-stress security incidents

Strategies for reducing panic and making better decisions during a cyberattack

You've been attacked. What's next?

In the midst of a ransomware attack or other such cybersecurity incident, emotions at the affected organization run high — playing right into the hands of attackers who thrive on creating a state of chaos, urgency and fear to accomplish their goal of monetizing the attack. The emotional state of people involved in the response can significantly impact the effectiveness and speed of recovery, including key decisions about whether to pay the ransom and how to restore systems.

To understand how ransomware attacks and other security incidents can place business operations and employees under immense stress, put yourself in this scenario.

Imagine that you are responsible for a global manufacturing organization. It's late on a Friday evening, before a public holiday, and your company's year-end report is due in 2 weeks. Your phone rings. It's your chief information security officer (CISO), who says, "We have a crisis — we're locked out of servers around the world. We can't get past screens that say our systems will be owned and encrypted until we pay a ransom demand. They are threatening to publish our customer data, and they say they have copies of our latest product designs!"

The situation is chaotic. SAP and line-of-business solutions can't be accessed. Identities have been compromised. The on-call service desk lead needs advice on how to respond to the situation. Production lines are shut down. You cannot pay suppliers or run year-end reporting. Your payroll is at risk. Even worse, your business continuity plan (BCP) is on one of the impacted servers. The stress level is high, and rising.

DXC Technology has helped many global companies and public sector agencies respond to and recover from ransomware attacks, as well as harden environments against threat actors' tactics and techniques. A globally leading security services provider, DXC routinely performs post-incident reviews with customers to identify lessons learned and implement recommended improvements.

One key takeaway, relevant to every organization, is the importance of anticipating and proactively addressing the emotional impact on incident response teams of these high-stress attacks. This paper discusses ways to emotionally prepare response teams for responding to cyberattacks, and for protecting team members' well-being.

Emotional model for operational crises

To understand the emotional experiences of incident response teams, let us turn to psychology. We have adapted the model for the stages of grief, as described by Swiss-American psychiatrist Elisabeth Kübler-Ross, to focus on key factors that influence the intensity of emotional phases during a security incident (see **Figure 1**).

The six phases of emotional response are denial, panic, frustration, depression, acceptance and return to normal. We will describe the emotional roller coaster of these phases and explore ways that incident responders can move as quickly as possible through less productive phases and shorten the time between frustration and acceptance.

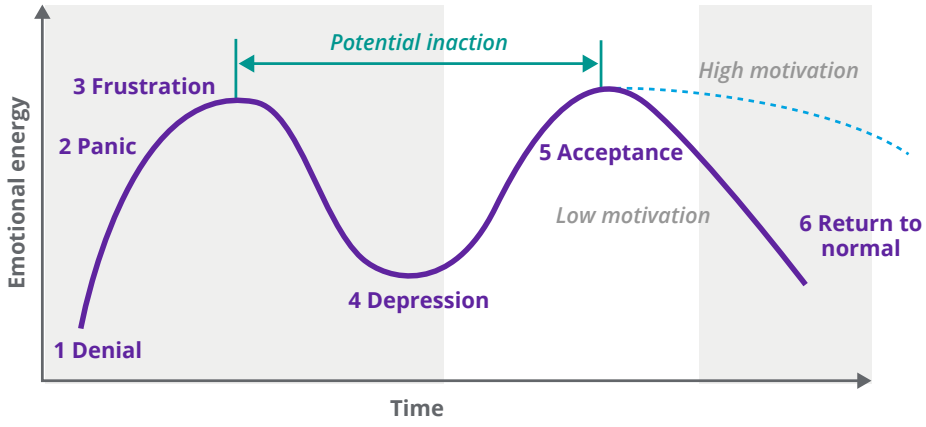


Figure 1. Emotional phases during a security incident

Phase 1 — Denial

Various behaviors that fall under the umbrella of denial can exacerbate a crisis situation. For example, certain unusual activity may initially go undetected, when the root cause diagnosis and corresponding response plans are not yet in place.

Threat actors may have access to an environment for some time before their activity is detected. During this time, they move laterally, elevate privileges, create backdoors and hide their presence. After the fact, forensic investigations often find that security monitoring tools detected suspicious activities or strange event patterns, but these were either not flagged or not fully investigated.

Another denial behavior relates to focusing analysis and countermeasures only on a specific resource or component where the event is detected. If, for example,

Denial can lead to reluctance to accept indirect evidence of a major security incident.

a local administrative account has been compromised, only this specific account is deleted, or its password reset. Too often, operational teams tend to assume a situation is less pervasive — and therefore less impactful — than it really is.

By minimizing the problem, organizations are less likely to escalate the event to internal or third-party incident response teams, which could otherwise evaluate incidents with threat intelligence and threat-hunting capabilities.

Even when an incident has been identified and there is a clear, significant operational impact, teams can also demonstrate denial by assuming the problem is related to a component failure. The typical reaction is to replace and/or recover the affected component(s) and carry on. However, this approach ignores the special complexities prevalent in security incidents, where the scope of the infection may be unclear. Restoration may alleviate initial symptoms but not provide a cure, often resulting in a system becoming reinfected within hours of coming back online.

Finally, denial can lead to reluctance to accept indirect evidence of a major security incident. Time may be spent looking for other explanations for the incident, while the threat actor continues to mine, encrypt or damage operations — with potentially severe consequences,

Counteracting the denial phase

We have found that the intensity and extent of the denial phase is related to the security maturity of the organization, the team's understanding of the event and its impact. The goal is to get through this phase as quickly as possible and to ensure the appropriate transparency and flow of information. The activities or actions to ensure emotional preparedness to do so can be proactive, reactive or both.

Proactive actions

- Increase security awareness and instill a cultural change around information sharing.
- Define a holistic enterprise security policy and enforce it technically and organizationally.
- Implement technical controls that support infrastructure resilience.
- Include all areas of enterprise architecture, from networks to applications, in threat alert and resilience roadmapping.

It is essential to deliver on actions that have been committed to. Effective responses require an open-door policy for escalations and suggestions.

Reactive actions

If things do not run as expected even with proactive plans in place, improved communication and setting the right expectations, then it is essential to deliver on actions that have been committed to. Effective responses require an open-door policy for escalations and suggestions.

Phase 2 — Panic

Panic builds as the extent of the impact becomes clear. Stress within operational support teams grows as activities begin to fan out across various technical and organizational tracks. The natural response is to try to exert some control over the situation, even if activities are unplanned and unstructured. Several factors can exacerbate the situation:

The natural response is to try to exert some control over the situation, even if activities are unplanned and unstructured.

- "Boil the ocean" approach — the inclination to try to make progress on everything, in parallel with a lack of resource prioritization
- Limited or out-of-date support artifacts — unanticipated failures of the BCP related to critical documentation and other elements of the configuration management database (CMDB)
- Indiscriminate time pressure from the business
- Insufficient understanding of the scale of the incident, often driven by denial behaviors

At the same time, the number of meetings and people participating in them diffuses efforts, further builds the sense of being out of control and increases the level of stress and panic.

Counteracting the panic phase

Higher levels of maturity and preparedness reduce panic; a mature, prepared organization can leave the panic phase faster and move into more productive phases. This increases confidence and enables fast and effective decision making — in turn, accelerating the organization's ability to regain control of the environment.

Participate in tabletop simulations and other training exercises to understand the decisions that must be made and the nature of the questions that may arise.

In addition to technical preparedness, DXC recommends that teams participate in tabletop simulations and other training exercises to understand the decisions that must be made and the nature of the questions that may arise. Another crucial preparation activity is clearly defining the matrix of roles and responsibilities, and creating associated diagrams for responsible, accountable, consulted and informed (RACI) decision-making, as well as incident response playbooks or checklists.

Documentation that is discussed, defined and planned in advance helps to reduce panic-mode operations.

Phase 3 — Frustration

Frustrations can result in further communication breakdowns, widening divisions within the team and potentially leading to a siege mentality and poor practices.

The frustration phase stems from the diffusion of effort in Phase 2 and contributes to confusion in communications and a perceived lack of progress. As soon as the organization commits to a recovery schedule, teams will be under even more pressure from stakeholders, including executives and affected customers, regulatory bodies and other external parties.

During this phase, the operations team typically gets a clearer understanding of the extent of the incident and the scale of the remediation effort. Some systemic issues may surface, including poor credentials hygiene, outdated or end-of-life systems and software, limited patching and weak administrative practices — triggering additional remediation and improvement activities.

These frustrations can result in further communication breakdowns, widening divisions within the team and potentially leading to a siege mentality and poor practices.

In parallel, the intensive work pattern continues. At this point, response team members may have devoted 60+ hours to the incident, with little or no sleep.

Counteracting the frustration phase

The search to answer the question "How did this happen?" will be on everyone's mind, but immediately launching an investigation can divert key resources from essential evaluation and recovery activities.

It is completely understandable for response teams to feel frustrated by all the unwelcome news, and management teams should ensure that post-incident discussions address questions about responsibility and ethics. However, these sessions should happen after the situation is back to normal.

The search to answer the question "How did this happen?" will be on everyone's mind, but immediately launching an investigation can divert key resources from essential evaluation and recovery activities. Root cause analysis is a useful technique; however, pinpointing the full extent of causes could take weeks, or could be impossible to determine. Overemphasizing the search for causes can lead to a hunt for blame, and deflection of responsibility, or attempts to appear productive and demonstrate progress. Raising suspicions of a potential internal threat actor could further heighten the tension and potentially lead to a witch-hunt, increasing negative emotions and mistrust.

Well-prepared organizations following a pragmatic plan can reduce frustration and even derive positive results from the crisis. We have seen customers, partners and key stakeholders praise organizations hit by severe incidents for ensuring strong communications and decisive actions during the crisis.

To help minimize frustration, leadership teams should address resource demands. Balance capabilities across various teams through effective shift planning and a follow-the-sun staffing approach that can reduce levels of stress and fatigue.

Getting assistance from a global security service provider such as DXC offers a clear advantage in terms of having processes and resources in place to support around-the-clock, personnel-intensive activities.

Phase 4 — Depression

Dwelling on “if only we had” scenarios fuels negative self-evaluation and emotional spirals of depression.

Depression can set in when the full impact and realistic recovery timeframe are known. During labor-intensive rebuild activities, things typically don’t go as expected. The recovery of complex systems is complicated and time consuming, and teams may be tempted to take shortcuts or accept elevated risks to gain quick wins.

The nature of the incident also may require changes to the disaster recovery (DR) plan, resulting in several false starts by this point. Response teams, including management, understand the full extent of the upcoming material impact for the organization and realize there is no silver bullet for recovery. Dwelling on “if only we had” scenarios fuels negative self-evaluation and emotional spirals of depression.

These challenges and additional pressure related to legal requirements and business needs usually come as a surprise to the leadership team and can lead to a lull in activities.

Counteracting the depression phase

During the depression phase, it is especially important to maintain motivation, improve morale and continue to look for tactical improvement possibilities. Team members will be exhausted, and if the team’s workload is not addressed proactively, this problem will accelerate the decline in motivation and morale.

The best way to move beyond this phase is concrete prioritization and guidance on how to approach the various challenges. Distributing the workload across day and night shifts — and ensuring teams have roughly equal skills and experience — favorably impacts the overall situation. As a rough estimation, at the beginning of the incident (first through sixth day), the night shift’s efficiency is generally at 40 to 50 percent of the day shift’s efficiency. This improves in later stages of the recovery activities, with night shifts reaching 70 to 80 percent of the day shift’s efficiency. Efficiency also can vary between time zones.

It is important to push motivating communications to these teams as swiftly as possible. Focus on tactical improvements that document positive progress to the teams and management.

It is important to push motivating communications to these teams as swiftly as possible. Focus on tactical improvements that document positive progress to the teams and management. These communications help drive a faster transition to the acceptance phase.

Phase 5 — Acceptance

In the acceptance phase, the incident management and remediation teams are working at maximum efficiency. The scale and scope are understood; the remediation and recovery plan has been defined, validated and executed; and communication paths are established and functioning. The aim of the BC/DR plan

should be to reach this state of optimum team performance as soon as possible. In the best case, remediation and recovery plans have been reviewed, tested and approved through tabletop exercises conducted prior to any incident. Effective plans should include considerations of future strategic initiatives and support for future approaches.

The organization and its management should focus on establishing and maintaining a positive unified spirit and use this momentum to address critical issues with optimal efficiency.

Supporting the acceptance phase

As acceptance is the most effective phase, the organization and its management should focus on establishing and maintaining a positive unified spirit and use this momentum to address critical issues with optimal efficiency.

Phase 6 — Return to normal

The announcement of the return to normal operations should mark a happy conclusion of incident response and recovery activities. The adrenaline rush of the high-stress situation is over. The state of normalcy is welcomed by all, along with a sense of relief. All too often, however, this milestone could lead to feelings of complacency that may have led to the original crisis.

This phase is a true test of lessons learned and the organization's commitment to improving its security posture. Motivation for investing in security-related activities can decline as leadership teams focus on immediate post-incident business needs. Often, leaders feel they have spent long enough on security and need to turn to more business- and revenue-related priorities. This attitude can send the wrong message to the organization, fostering a perception that the danger has passed.

Proactive remediation efforts followed during the incident tend to fall off or revert to the pre-crisis state.

For security and IT teams, proactive remediation efforts followed during the incident tend to fall off or revert to the pre-crisis state. The heightened focus on remediating vulnerabilities, increasing capabilities and establishing more efficient processes will inevitably wane as time passes, and eventually, employees could feel overwhelmed by the enormity of the effort. Complacency sets in — until another security incident impacts the business.

Building on the return-to-normal phase

The response team needs to commit to and develop an information-based security improvement strategy that covers relevant areas of improvement — including prioritization and risk estimation.

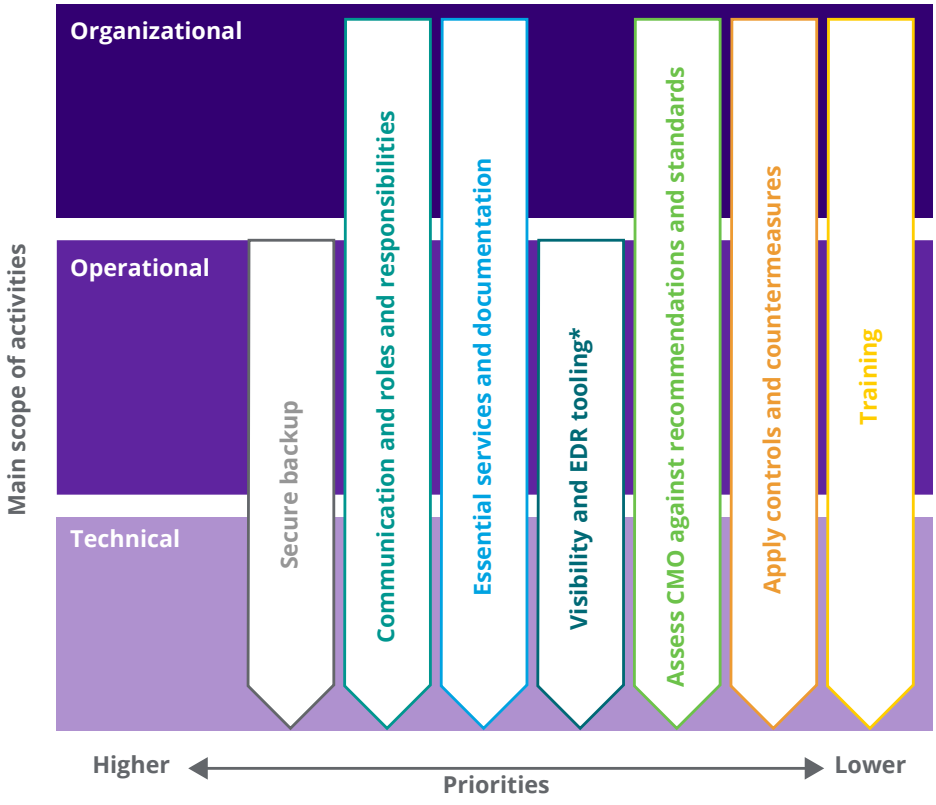
To build on the organization's return to normal, the response team needs to commit to and develop an information-based security improvement strategy that covers relevant areas of improvement — including prioritization and risk estimation. Information collected during the forensic investigation further informs this improvement plan. Organizations with low levels of maturity should conduct regular educational sessions on security administration.

It is important to connect the outcome of the incident and recovery plan to broader corporate governance. Functions such as audit committees and board oversight need to be leveraged to establish proper and consistent follow-up activities, including KPI-based reporting.

Strategies to address negative emotional responses

Preparing team members for an incident can positively impact the overall recovery experience and results. Unfortunately, BCP and DR processes often do not sufficiently address the potential for crippling attacks such as ransomware, which contributes to negative emotional responses.

Figure 2 shows the main scope of IT in enterprise environments, including proactive controls and countermeasures, with activities prioritized from left to right. Based on an organization's specific industry, capabilities and maturity, the amount of effort for these preparations may vary. The level of need can usually be evaluated through a cybermaturity assessment directly linked and aligned with BCP and DR planning activities.



* EDR: Endpoint detection and response

Figure 2. Key preparation areas for security incidents

We believe the most important goal should be to articulate complex situations in an easy-to-understand and structured way.

Culture is another issue that cannot be underestimated — especially if an organization operates globally. Regional differences regarding how to handle crisis situations and urgent tasks must be addressed within the policies and culture of the enterprise.

Work during the recovery phases will always be intense, but the intensity of any situation can be reduced with better planning, preparation and coaching.

How to reduce the impact of attacks

Ransomware and other destructive attacks will continue to be an issue. These threats are not specific to any region, industry or technology. Based on our experience, an awareness of the emotional response at various stages — and proactive preparation to manage the response emotions — can help reduce the impact of such events.

If you have not yet reached out to your trusted advisors and service providers, now is the time to do so. Be sure to include topics such as emotional response on your agenda when planning your response activities.

A crisis has a significant emotional impact on analysis and recovery activities. Work during the recovery phases will always be intense, but the intensity of any situation can be reduced with better planning, preparation and coaching.

DXC has published two technical guides to support these activities:

- Proactive — **Ransomware defense guide: Prepare for an attack**
- Reactive — **Ransomware survival guide: Recover from an attack**

The following approaches can help to reduce stress and improve efficiency:

- Know your infrastructure and keep an up-to-date and correct CMDB. You can only protect what you know about.
- Ensure that monitoring and endpoint detection and response tools are in place. Your organization needs alerts as early as possible to detect suspicious patterns and isolate risky systems.
- Review incident management and business continuity plans regularly. Cyberthreats, from IP exfiltration to destructive attacks, must be addressed in these plans.
- Adopt all resources that can speed response activities before a crisis happens. You'll need the names of key stakeholders and their contact information, RACI diagrams, and third-party vendor contacts and support agreements. Also critical is having a good understanding of essential business services needed for the survival of the organization, and timelines required to secure the business.
- Understand all technical dependencies — storage requirements, network bandwidth, and rebuild, clean and recovery durations — because these aspects will have a significant impact on the overall timeline.

Finally, don't lose sight of what happened — this can occur in the emotional jubilation that takes place after full recovery. Reflect on the event, and apply your momentum to assume a better security posture to prevent the possibility of any recurrence — and avoid more sleepless nights.

How DXC can help

Cyberattacks can be disastrous to an organization and its reputation. DXC is well positioned to guide customers through all of the emotional phases and ensure a timely and positive return to normal business activities. DXC leverages global services and more than 3,000 security experts who protect some of the world's largest enterprises to reduce risk and respond to attacks.

About the author

Lars Klinghammer is director, cybersecurity architect and global remediation lead in the Security practice at DXC Technology. With more than 25 years of experience in security consulting, he helps businesses proactively improve security, respond to attacks and recover the IT environment. Previously, he was a global cybersecurity architect in the Microsoft Cyber Security Global Practice, where he helped customers improve identity and access management, secure environments and implement security improvement plans.

Learn more at
dxc.com/security

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.