



The future of incident management

Why organizations need to take a different approach



Introduction

Incident management isn't new — systems have been breaking and organizations have rushed to fix them for a long time. However, expectations for great customer experiences are rising along with intense competition for digital market share. Companies must release features quickly to remain competitive, but it can be difficult to balance development velocity with reliability and performance. This reality is forcing organizations to improve their incident management processes to keep pace with their digital services.

Imagine you're a service owner in a company that has just released a new digital service. Your service is a success, but perhaps too much so. Your help desk has alerted you that customers are complaining about poor page loading times. You need to resolve the issue quickly, so you get to work troubleshooting:

- Suspecting that an underprovisioned database cluster is to blame, you **check the #dba channel in Slack** to see who is on call.
- Meanwhile, you create a **conference bridge** and post the details in the #dba channel.
- Your **CEO calls you** to ask for information on how impactful the issue is. You don't know yet.
- The **Database Administrator (DBA)** on-call then reports that you've accidentally provided the host instructions for the conference instead of the participant code and invitees can't get into the bridge. You quickly correct your mistake and the DBA joins.
- You ask the DBA to give the database cluster more resources, but they can't do that without a change ticket. You create a **change ticket** and the DBA makes the change.
- The added database horsepower has no effect — it looks like this isn't a database issue after all. Your DBA remembers that an issue like this happened exactly two weeks before at this time but there is **no record** of the details.
- You're now **17 minutes** into this degradation and you're no closer to a fix.
- Your CEO calls you to ask you for an estimated time to resolution. **You don't know yet.**

The impact of service degradation is undeniable

A recent study shows that [47% of consumers expect a web page to load in 2 seconds or less.](#)

Facebook's 2021 outage that lasted only six hours cost the company

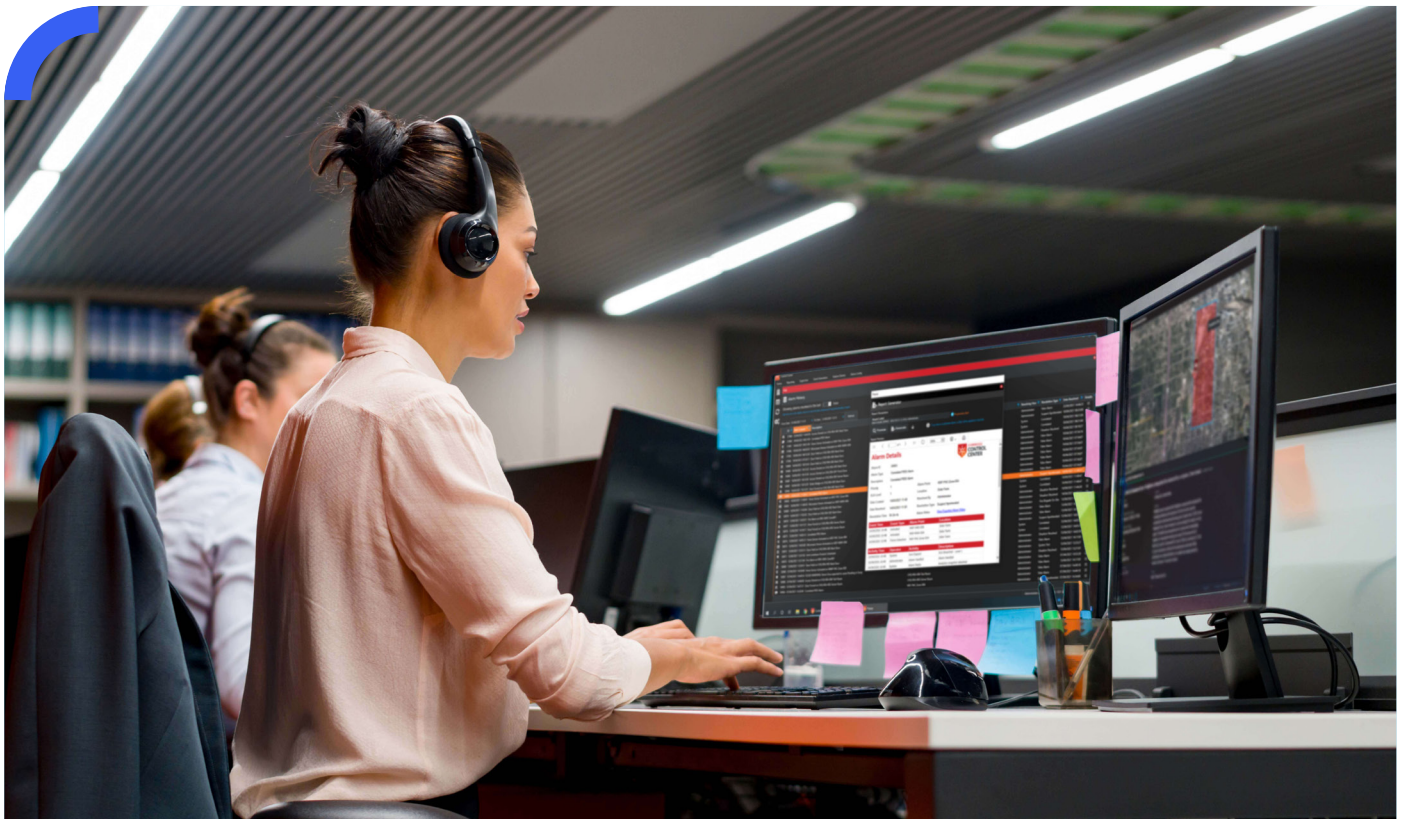
\$164,000
a minute in revenue.

The well-intentioned but ad hoc approach to incident management described above is inadequate in today's high-stakes environments. Regardless of process type, anyone who has been in the trenches trying to resolve issues will recognize the associated problems, delays, and frustrations outlined below:

- Waiting for customers to tell you that there is an incident means that the impact started before responders were even aware that there was a problem.
- Manual tasks like creating conference bridges and opening tickets leave room for errors and further wasted time.
- Not having records of past incidents virtually guarantees that history will repeat itself.
- Having ill-defined communication channels for engaging responders and updating stakeholders means the incident commander is losing valuable cycles switching between channels and fielding inbound requests for information.

The impact of poor incident management

The impact of poor incident management cannot be overstated. Outages, performance degradations, application errors, and other types of incidents must be resolved quickly to keep customers engaged — and to avoid low NetPromoter Scores (NPS) and customer churn.



The incident management spectrum

Organizations vary in their approaches and maturity levels in supporting their services.

Ad hoc	Traditional	Modern
<p>Smaller and newly-formed companies often lack a formal incident management process. Instead they rely on customer-reported outages to become aware of incidents. Spreadsheets are used for on-call scheduling and email is used for communication and collaboration.</p>	<p>This approach combines service desks with strict processes to triage and resolve incidents.</p>	<p>This approach combines manual and automated processes to resolve incidents. It employs issue tracking tools, monitoring platforms, and chat applications to respond to alerts and notifications. Individual teams are tasked with detecting and resolving incidents for the specific services they manage.</p>
<p>As customer demand increases, these organizations struggle with:</p> <ul style="list-style-type: none"> • Engaging the right people quickly. • Notifying stakeholders about impact. • Facilitating collaboration among incident resolvers. • Evaluating how much incident management is costing the organization as a whole. • Keeping records of past incidents. • Learning from past failures. 	<p>These organizations struggle with:</p> <ul style="list-style-type: none"> • Resourcing for a high volume of incidents combined with a heavy process. • Resolving incidents quickly, due to handoffs between tiers and teams. • Involving too many people in major incidents. • Focusing on customer experience due to lack of alignment. • Using lowest-common denominator tools chosen by committee. 	<p>Still, some challenges persist:</p> <ul style="list-style-type: none"> • Lack of coordination between individual service teams and centralized incident management groups. • Automation limited to on-call engagement and collaboration channel creation. • Variable processes make it difficult to evaluate incident response consistently. • Poor visibility into engaged resources, and difficulty in engaging further resources as the situation evolves.

Adaptive incident management

There are critical challenges associated with all of these approaches, but everyone agrees that there is great value in being able to resolve incidents faster to provide an outstanding customer experience. This is the goal of adaptive incident management.

Organizations need a platform that integrates a variety of cultures, toolsets, architectures, and methodologies to provide consistent, efficient and measurable incident management.

The term adaptive is used in multiple contexts:

To overcome the challenges inherent in the previous approaches, incident management practice needs to scale incident response according to the situation, incorporate automation where ever possible, accommodate a variety of tools and cultures to support resolvers, and collect data to fuel continuous improvement.

Scale

Adaptive incident management should be able to adapt based on situational awareness of the incident. It should be able to scale up and down as the situation demands, which can mean:

- Engaging additional resolvers, or dismissing resolvers that are no longer needed.
- Providing appropriate automated resolution tasks depending on the nature and status of the incident.
- Facilitating appropriate collaboration, from a single team chat channel to multiple conference bridges and status pages for resolvers, stakeholders, executives and vendors.

Tools & cultures

Adaptive incident management should be able to adapt to a changing landscape of tools and departmental cultures. The ability to provide open and flexible tool choice is important for a number of reasons:

- The ecosystem of tools is constantly changing, and adopting the latest technologies can result in a competitive advantage.
- Giving service teams the autonomy to choose the best tools for their particular service means they can be as efficient as possible and develop pride of ownership.

Adaptive incident management should also be able to bridge different cultures within an enterprise. Allowing different groups within an organization to stay within their tool of choice means they can work efficiently whether their workflow is based on a chat system, service desk, CRM system, or otherwise.

Similarly, these groups may have different methodologies including DevOps, SRE, ITIL, or ICS. And since most organizations have defined standards, integrating with tools that are part of the corporate mandate can save responders precious time so that they can focus on resolving an incident rather than checking boxes to adhere to standards.

Continuous improvement

Finally, an adaptive incident management practice should itself adapt over time by facilitating continuous learning. This is achieved by normalizing data across a variety of teams and tools, keeping records of all important events during the course of incident resolution, and facilitating post-incident retrospectives so that organizations can continuously improve their incident response.



FEMA's Incident Command System (ICS)

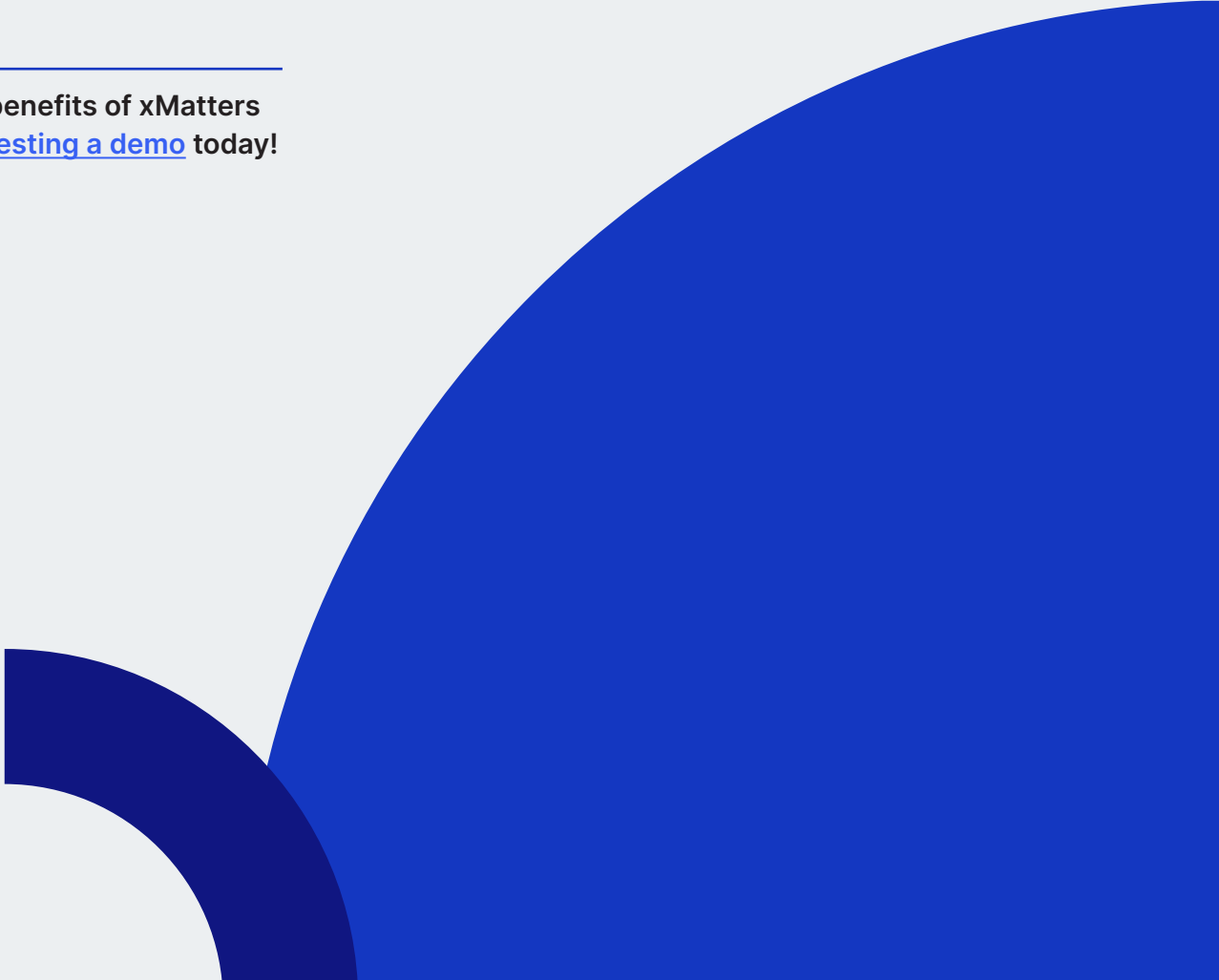
One methodology supported by adaptive incident management is FEMA's Incident Command System (ICS), which creates a clear chain of command during an incident. The system begins with a state of chaos, identifies the cause of the incident, fixes the problem, and then evolves and streamlines the process with each new incident.

If executed properly, the system establishes a clear inventory of the resources available so the incident commander can efficiently deploy resources. With digital services, the challenges aren't physical, but the processes and best practices learned from FEMA can be applied to the digital world. Several ICS best practices have been identified and incorporated into the Site Reliability Engineering (SRE) handbook.

Summary

Incident management is changing. While it was once a well-defined process in the IT organization focusing primarily on service availability, it has evolved to embrace DevOps and SRE practices, with an added focus on service performance. Because business success is now driven by customer experience, diverse teams need to work together to increase engagement, reduce churn and deliver the digital services people rely on. Organizations practicing traditional — and even modern — incident management must evolve their approach to address issues systematically. This includes increasingly leveraging data and automation while facilitating the power of human collaboration and continuous improvement. **We call this practice and process evolution adaptive incident management.**

Experience the benefits of xMatters
yourself by [requesting a demo](#) today!





About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) empowers enterprises and government organizations to anticipate, mitigate, respond to, and recover stronger from critical events. In today's unpredictable world, resilient organizations minimize impact to people and operations, absorb stress, and return to productivity faster when deploying critical event management (CEM) technology. Everbridge digitizes organizational resilience by combining intelligent automation with the industry's most comprehensive risk data to Keep People Safe and Organizations Running™.

For more information, visit Everbridge.com, read the company [blog](#), and follow us on [LinkedIn](#) and [Twitter](#).

[Get in touch](#) to learn about Everbridge, empowering resilience.

