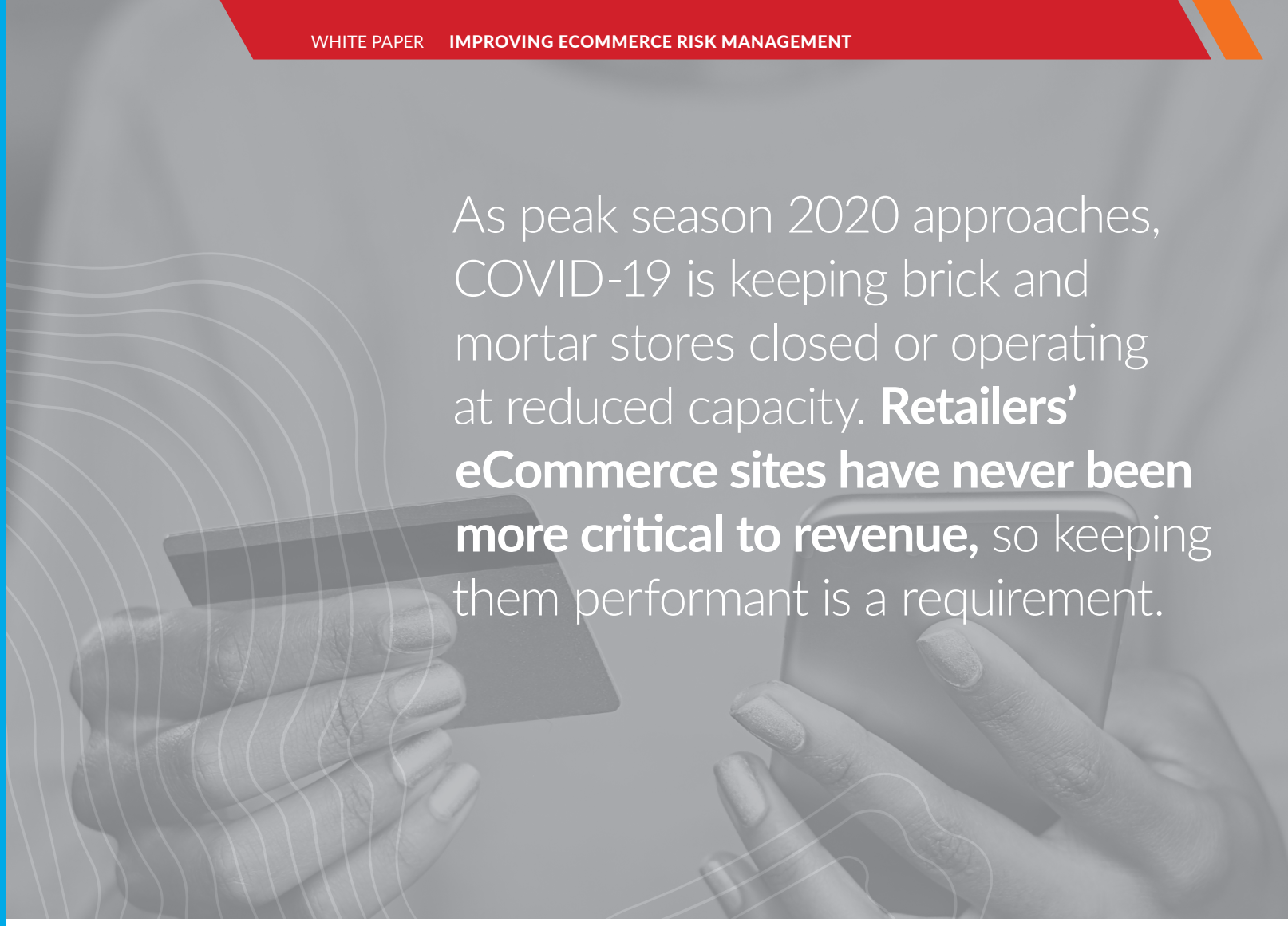
everbridge®

Improving eCommerce Risk Management:

Enhancing MTTR with a Flexible Response Plan



As peak season 2020 approaches, COVID-19 is keeping brick and mortar stores closed or operating at reduced capacity. **Retailers' eCommerce sites have never been more critical to revenue,** so keeping them performant is a requirement.

eCommerce has never been as critical for retailers as it is in 2020. According to Adobe Analytics, year over year eCommerce sales grew 76% in June, from $41.5B in 2019 to $72.2B in 2020. Peak shopping season is approaching, but COVID-19 continues to impede store operations. Companies like Walmart have already announced that they will close for Thanksgiving; in fact Walmart is rumored to be preparing a competitive online service to Amazon Prime.

This unprecedented, rapid consumer shift to online buying puts the reliability of retailers' eCommerce sites front and center to their leadership teams. As demand increases, consumers place greater stress on online platforms, exposing design flaws and performance issues. Despite the best efforts of ecommerce retailers, many of their sites will experience performance degradation or even failure at some point during a peak demand period. This causes unnecessary and excessive damage to the business in the form of reduced sales, customer satisfaction and brand equity.

This is not news to those responsible for keeping their sites up and running. However, what may be news to them is how the increasing demand on and complexity of ecommerce sites makes it more and more difficult to prevent the problems that can slow or crash customer-facing services. In addition to trying to prevent these issues, retailers need to improve their ability to respond to the issues that inevitably occur despite their best efforts so they can minimize their impact on the business.

One bottleneck many ecommerce organizations pay too little attention to is the delay between detecting an issue and assembling the appropriate team members, wherever they are inside or outside the organization, allowing them to collaborate and orchestrating their work to resolve the issue. Read on to learn how such delays hurt the business and how an agile, flexible communications strategy can slash the time required to get an ecommerce site back up and operating when it matters most.

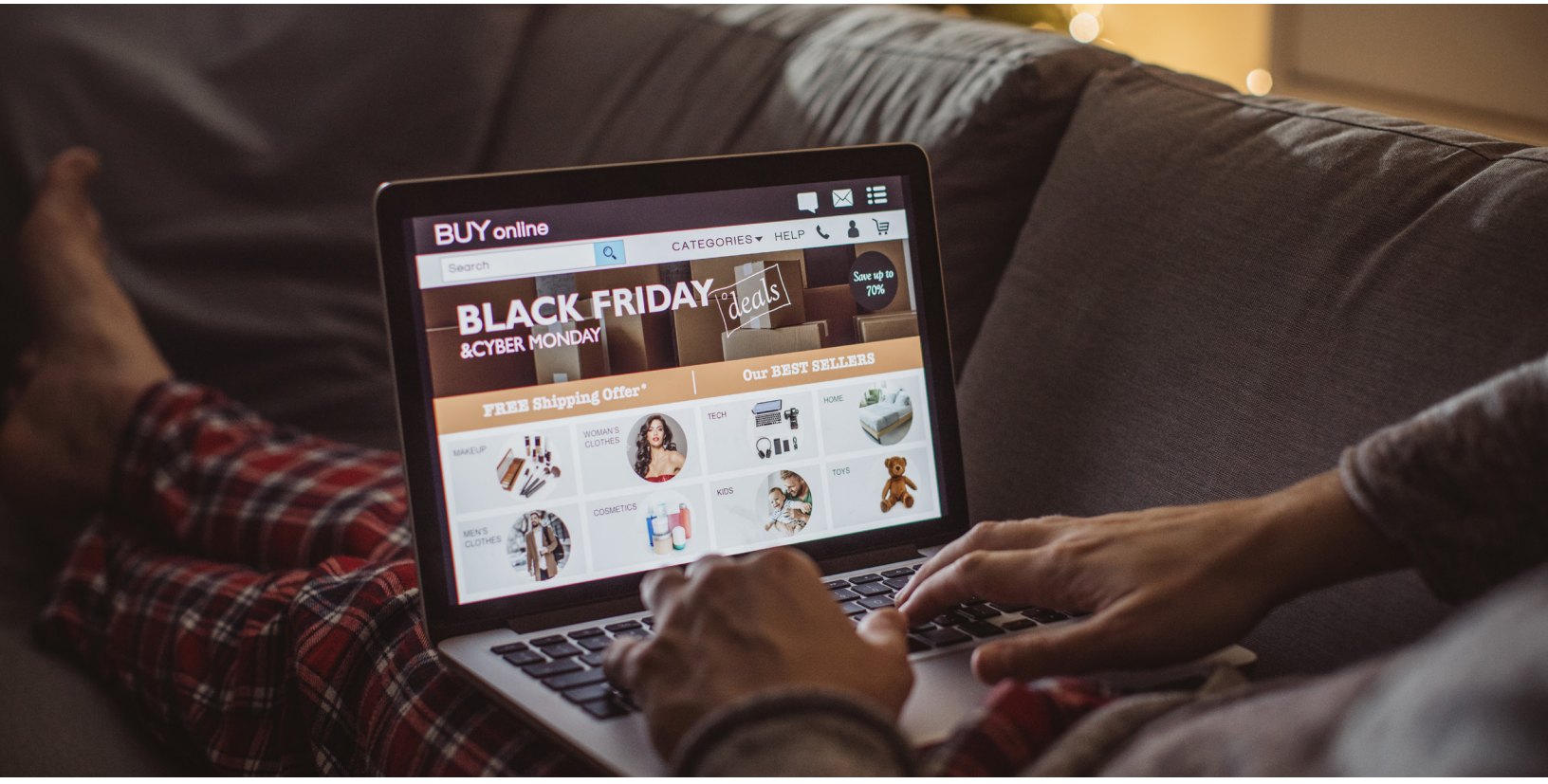
Plan to Fail

All retailers know they should plan to avoid IT outages during peak demand periods. That's when their systems will be under maximum stress, and when slowdowns or outages will cause the most damage in the form of lost revenue, lower conversion rates, higher customer churn and damage to their reputation.

24.3%
of online merchants experienced five minutes or more of downtime during 2019 Black Friday and Cyber Monday.

More than 36% of e-commerce professionals surveyed by Webscale say their online storefronts generate as much as half their annual revenue in the fourth quarter. But 24.3% of online merchants experienced five minutes or more of downtime during 2019 Black Friday and Cyber Monday, while nearly 50% experienced page load times of more than 3 seconds. Such slow response times are intolerable when site performance is such a key metric of customer satisfaction and conversion.

Even the operators of the biggest ecommerce sites can be brought down by their own infrastructure. An hour after the start of the July 2018 Amazon Prime Day sales event, "errors were coming up at checkout, items in shopping carts were disappearing, mobile



alerts were delayed, products searches were sometimes offering no results, and some shoppers were caught in a 'Shop All Deals' loop," reported technology site CNET.[1]

News channel CNBC quoted internal Amazon documents showing that a system used to provide computation and storage services to multiple Amazon businesses, including Prime, failed to secure enough servers to handle the traffic surge.[2]

Among the third-party services that have caused serious problems is Cloudflare Inc., an internet service designed to speed and protect Web sites. A misconfiguration of its Web application firewall in July 2019 caused a global outage that crashed sites including Shopify's ecommerce platform and blogging platform Medium.[3]

When an outage does occur, corporate PR and marketing must be able to control the notifications and updates shown to the affected customers. Otherwise, a bad situation can be made worse by misleading messages, such as that posted by clothing retailer J Crew after a 2018 Black Friday outage saying, "Hang on a sec… you'll be able to get back to shopping shortly." According to Web site monitoring vendor Uptrends, "the 'sec' ranged from 30 seconds to several minutes."[4]

1. CNET: Amazon.com suffers outages at start of Prime Day 2018 https://www.cnet.com/news/its-not-just-you-amazon-appears-to-be-down-on-prime-day/
2. CNBC: Internal documents show how Amazon scrambled to fix Prime Day glitches. https://www.cnbc.com/2018/07/19/amazon-internal-documents-what-caused-prime-day-crash-company-scramble.html
3. Bloomberg News: A massive outage takes down Shopify sites, Bloomberg News | Jul 2, 2019, https://www.digitalcommerce360.com/2019/07/02/a-massive-outage-takes-down-shopify-sites/
4. Uptrends: Black Friday 2018: Best & worst website performance & uptime. https://blog.uptrends.com/uptrends-research/black-friday-cyber-monday-2018-best-worst-website-performance-uptime/

Having a plan to quickly detect, respond, investigate, fix and test (DRIFT) issues, and the right technology to support that plan, is critical when preparing for peak sales periods.

Minimizing such damage is why having a plan to quickly detect, respond, investigate, fix and test (DRIFT) issues, and the right technology and processes to support that plan, is critical when preparing for peak sales periods. Most retailers have invested in the detect, investigate and fix processes, but not in minimizing the time between the detection of an issue and making the right people aware of the issue and coordinating their work to resolve it. This can often constitute the greatest delay between detection and remediation, yet it receives the smallest investment, perhaps because retailers don't know that a solution exists in the form of modern alerting, communication and collaboration solutions.

The importance of speedy notifications, and the challenges of determining who needs to be notified, is rising due to the growing complexity of ecommerce sites, the range of potential problems they face and the number of partners that might be affected by an outage. An ecommerce Web site might offer products from multiple external sites and rely on third-party providers for everything from search to product catalogues to services such as DNS (domain name system) and content delivery. Their site can be slowed or stopped by a failure at any one of these providers, as well as by hackers attacking any of them.

All this makes it more important than ever to plan how to respond to incidents whose causes may not be immediately apparent, in addition to planning to avoid outages.

Flexible Communications

One area where many organizations fall short in their response planning is in communications, and especially the ability to find and communicate with business partners and stakeholders whose importance they did not realize before the incident.

For example, a typical incident response plan might provide for notifying:

+ The IT team about the outage and determining a cause and predicted time to resolve.
+ The security team to determine if the outage was caused by an attack and, if so, if data was breached.
+ Legal and audit groups to advise them if data was breached and whether their involvement is needed.
+ Regulators and industry groups to inform them if data was breached, even if only to assure them it was not.
+ PR and investor relations to tell them if data breached, even (again) if only to assure them it wasn't.
+ The social media team to update them out the issue and provide messaging it can publicize.
+ Store managers in the event of an issue affecting the omni-channel experience such as "Buy Online Pickup In Store."

All these steps, as essential as they are, don't cover the unexpected notification processes required by unexpected and unpredictable causes such as these:

Poor Patch Practices at a Third-Party Loyalty Program

If an ecommerce site crashes because the operations staff at a third-party loyalty program mistakenly brings down a critical server for patching during a peak sales period, the ecommerce provider must go beyond their planned notifications to also:

+ Establish communications with a troubleshooter that can identify an external rather than an internal issue.
+ Once the source of the issue is identified, contact the owner of the relationship with that third party to identify and contact the appropriate stakeholder at that partner.
+ Create the communication and workflow to ensure the problem is solved and will not occur again.
+ If other business units within the organization use the same third-party provider, inform them of the problem and its cause so they can advise their employees and customers of an expected time to remediation, and take steps to assure the problem does not occur again.

Miscoded Pricing at an External Marketing Partner

If an ecommerce site crashes because product prices or the formulae for calculating discounts or promotions were improperly coded by an outside marketing firm, the ecommerce provider must go beyond their planned notifications to also:

+ Determine which internal or external players could have coded these pricing values.
+ Determine which internal or external player actually coded the values.
+ Establish a communications and workflow process to ensure the coding errors are corrected.
+ Determine which other products, business units or marketing affiliates might be affected by these errors so they can advise their employees and customers.
+ Notify the marketing manager responsible for these products, to advise of lost sales due to calculation errors and ensure formulas for dynamic pricing or discounts are correct before re-coding them.

Unprotected Services at a Transaction Processor

If an ecommerce site suffers a theft of customer records due to a poorly secured server at a third-party transaction processor originally hired by a newly acquired subsidiary, the ecommerce vendor must go beyond its usual notification processes to also:

+ Find who at the newly acquired subsidiary contracted with and owns the relationship with the transaction processor.
+ Identify and find the contact information for the appropriate personnel at the transaction processor.

+ Identify which other business units within the enterprise, or at its marketing partners, might have used this transaction processor and notify them of the breach.
+ Identify and notify regulators in any other geographies the ecommerce site serves that need to be identified about the breach.
+ Establish and enforce workflows with all internal and external parties to assure the problem is fixed and will not recur.

A Robust Messaging, Collaboration and Orchestration Platform

In addition to expanding their existing outage response plans, ecommerce organizations need a robust, flexible technology platform plan that allows them to quickly find, contact and communicate with any responder, whether inside or outside of the enterprise, so they can work together as quickly as possible to restore normal site operations. Importantly, this program also needs to manage resource availability in the face of COVID-19.

Everbridge's IT Alerting meets these needs by enabling the communication, collaboration, responder schedule management and orchestration of all the processes across the enterprise required to quickly resolve outages and critical incidents during peak ecommerce periods. It integrates with leading ITOM, SIEM, APM, NPM, ITSM and DevOps tools. Every time a glitch is detected, the appropriate response plan can be automatically activated which will identify, contact and engage with the on-call response team(s), in minutes, wherever they might be. No alerts are ever missed with automated escalation of communications if team members fail to respond.

One-click access to international conference bridges and chatops channels allows rapid coordination, investigation and runbook automation to accelerate resolution. The solution captures post-incident debriefing and compliance audits to improve response to future events. It also streamlines communication with non-IT staff and key stakeholders, proactively notifies potentially affected business users so they don't open new tickets with the service desk.

Using Everbridge IT Alerting, leading retailers have significantly reduced disruptions, shrinking the time to rally response teams by 80% and cutting overall duration of incidents by over 50%, preserving millions of dollars of revenue and compensating for brick and mortar store losses during COVID-19.

About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications that automate and accelerate organizations' operational response to critical events in order Keep People Safe and Businesses Running™. During public safety threats such as active shooter situations, terrorist attacks or severe weather conditions, as well as critical business events including IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, over 5,300 global customers rely on the Company's Critical Event Management Platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes through the secure delivery to over 100 different communication devices, and track progress on executing response plans. The Company's platform sent over 3.5 billion messages in 2019 and offers the ability to reach over 550 million people in more than 200 countries and territories including the entire mobile populations on a country-wide scale in Australia, Greece, Iceland, the Netherlands, New Zealand, Peru, Singapore, Sweden, and a number of the largest states in India. The Company's critical communications and enterprise safety applications include Mass Notification, Incident Management, Safety Connection™, IT Alerting, Visual Command Center®, Public Warning, Crisis Management, Community Engagement™, and Secure Messaging. Everbridge serves 8 of the 10 largest U.S. cities, 9 of the 10 largest U.S.-based investment banks, 47 of the 50 busiest North American airports, 9 of the 10 largest global consulting firms, 8 of the 10 largest global automakers, all 4 of the largest global accounting firms, 9 of the 10 largest U.S.-based health care providers, and 7 of the 10 largest technology companies in the world. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, New York, San Francisco, Abu Dhabi, Beijing, Bangalore, Kolkata, London, Munich, Oslo, Singapore, Stockholm, and Tilburg. For more information, visit www.everbridge.com, read the company blog, and follow on LinkedIn, Twitter, and Facebook.

everbridge®

VISIT WWW.EVERBRIDGE.COM

CALL +1-818-230-9700