everbridge®

THE MISSING PIECE OF HIGHER EDUCATION IT INCIDENT RESOLUTION

THE TECHNOLOGY LANDSCAPE

Over a 12-month period that began in September 2017, Kaspersky Lab detected nearly 1,000 phishing attacks on 131 universities.[1] Higher education is consistently noted as one of the most vulnerable, highly targeted industries for cyber-attacks. Colleges and universities represent a gold-mine for hackers, with vast stores of personal information and expensive research along with a lack of control over thousands of devices accessing their network. Michael Borohovski, founder and CTO of Tinfoil Security, states, "Protecting schools is a lot harder than protecting corporations, mainly because you have to allow people to bring their own devices. While the attacks aren't novel, universities don't have strict control over the hardware and software that students and faculty use."

And it isn't just cyber-attacks. As schools are increasingly dependent on technology to collect applications, register students, plan lessons, conduct learning, administer tests, and grade assignments, ANY disruption to software or hardware systems can have a significant operational impact.

With notable IT incidents such as hackers accessing Applicant Tracking Systems (ATS),[2] research universities being targeted to either steal research directly or hack and blackmail researchers,[3] registration systems failing at the worst possible time,[4] or full, extended network failure due to aging infrastructure,[5] it is critical that your institution's incident resolution process is optimized, consistent and predictable at all points.

That process starts from the point of incident determination, whether through proactive monitoring solutions or complaints to the service desk, and encompasses the time it takes to respond, investigate the cause, fix the issue, and test or validate the resolution. Everbridge uses the acronym DRIFT (determine, respond, investigate, fix, and test) to represent the general elements that make up MTTR, taking laser-focus on the time and mechanics of the response component.

D.R.I.F.T.

One method of IT incident resolution that can provide context on optimization is the 5-step D.R.I.F.T. framework. These steps are:

1. **Determine**
2. **Rally & Respond**
3. **Investigate**
4. **Fix**
5. **Test**

Resource allocation for these steps follows a typical pattern across higher education institutions.

Budget is allocated for the IT management tools and systems necessary for the "Detect & Diagnose" step, primarily monitoring tools, application performance management tools, and logging tickets into an ITSM/ticketing systems.

Tools as well as human capital are invested in Investigate, Fix, and Test.

The "Rally & Respond" step is typically under-appreciated and under-resourced. This step involves the communication of information about the IT incident as well as the gathering of the human capital and other resources necessary for Investigate, Fix, and Test. Despite being the bridge between two areas of high investment and high cost, institutions most often rely on manual processes rather than automated solutions.

The ramifications and business impact of unoptimized Response is significant. The measure of the time taken to restore an IT service after a disruption or an interruption is the mean time to restore (MTTR). Forrester estimates that 70% of the overall resolution time (i.e MTTR) can be wasted during the "Rally & Respond" step, which means for all the money spent on tools and people, organizations are still failing at steps such as tracking on-call schedules, getting resolvers on conference calls, and reaching people on the proper devices via multiple modalities. The time wasted during unoptimized Response can be the difference between an incident resulting in the reputational harm that has downstream effects towards applications and admissions versus one that is minor and contained.

OPTIMIZED RESPONSE

So how can institutions know that their Response step needs improvement? Some key indicators are:

+ **Lack of system integration:** When a ticket is opened, a lack of system integrations creates extra workflow steps such as multiple logins and manual data entry that decreases efficiency.
+ **No Clear accountability:** During critical incidents, it is imperative that the right IT Staff, the 3rd party solution vendor, the key stakeholders be contacted in a timely manner. Without centralized contact, group, on-call schedule management solution, too much is wasted "finding someone to help".
+ **Communications are usually limited to email:** Contact paths are limited and messages are missed due to the different mechanisms in which messages are sent and received. Without adequate options for communication, time is wasted manually sending vital messages that are lost or ignored.
+ **You can't coordinate who's doing what (and who's not doing what):** Without proper tracking and message receipt confirmation, it is nearly impossible to engage the response or escalate to the next persons in line if primary don't respond. This leads to tasks not being completed in a timely manner or tasks overlap where multiple resources are unknowingly completing the same tasks.

+ **You have an overlap of communication systems:** Using several notification, alerting, communication systems creates noise, confusion and encourages the "spray and pray" models where notifications are sent to large undefined groups of potential helpers. This only leads to delays in the incident response process causing larger impact on the faculty. Th staff and/or the students.
+ **You have no easy way to escalate issues to the right team. Your team is overwhelmed with alerts and ignore/miss the important ones:** There is no automated message escalation which leads to valuable time being wasted manually looking through on-call schedules attempting to find the appropriate resource that is available at that time.
+ **You can't get everyone on a conference bridge quickly:** Complicated conference bridge access leads to wasted time spent looking for conference dial-ins and access pins.
+ **You have difficulty communicating with administrators, faculty, students, and external vendors:** Time is wasted communicating details of the incident to teams outside of the IT department such as faculty and external vendors.

FOR MORE INFORMATION ON THESE STEPS, READ 10 WHY REASONS YOUR IT INCIDENTS AREN'T RESOLVED FASTER.[6]

A CHANGING ACADEMIC LANDSCAPE

Technology will continue to change how students are taught and how colleges and universities are run. Predictive analytics can match support systems with students for early intervention. Virtual reality will be integrated into the learning toolkit. Blended, low-residency, education will continue to grow, increasing the reliance of online access. The reliance on software and hardware will continue to grow, and the ability to resolve system incidents will be critical to the mission of the institution. Bringing information from your diagnostic tools to your resolvers as quickly and efficiently as possible will help your students, faculty, and bottom line.

[1] https://www.kaspersky.com/about/press-releases/2018_pr-scholars-phishing

[2] http://www.thesandb.com/article/admissions-system-compromised-in-hack-student-social-security-numbers-compromised.html

[3] https://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821

[4] http://www.thesandspur.org/students-plagued-by-class-registration-issues/

[5] https://www.insidehighered.com/news/2019/02/21/almost-week-no-internet-amherst-college

[6] http://go.italerting.com/incident-resolution-inefficiencies

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 to 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 4,500 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 2.8 billion messages in 2018 and offers the ability to reach over 500 million people in more than 200 countries and territories, including the entire mobile populations on a country-wide scale in Australia, Sweden, the Netherlands, the Bahamas, Singapore, Greece, 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 9 of the 10 largest U.S. cities, 9 of the 10 largest U.S.-based investment banks, all 25 of the 25 busiest North American airports, six of the 10 largest global consulting firms, six of the 10 largest global auto makers, all four of the largest global accounting firms, four of the 10 largest U.S.-based health care providers and four of the 10 largest U.S.-based health insurers. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Beijing, Bangalore, Kolkata, London, Munich, Oslo, Stockholm and Tilburg.

everbridge®

VISIT WWW.EVERBRIDGE.COM
CALL +1-818-230-9700