# AccumeView: Executive Cybersecurity Pulse

The monthly executive review is intended to keep you informed of recent threats that can impact the confidentiality, integrity and availability of your data and information systems so that your institution can make the necessary technical and procedural changes to protect your institution.

## Perspective: state of the marketplace

In a recent survey, Nearly **Half of IT Execs** interviewed stated that they don't rethink or retool their approach to security after an attack, almost ensuring another attack in the near future. A critical step in the remediation of a security incident is determining what elements require change so that the incident won't repeat itself. A mature IT organization will ensure that this step is never skipped: immature organizations are destined to have history repeat itself.

A Nigerian threat group involved in **business email compromise** (BEC) named GOLD GALLEON has recently been uncovered. Their success ($6.7 million per year) underscores the severity of BEC attacks compared to other types of social engineering. A successful BEC attack leverages faults in security awareness **and** business processes. Be sure that your organization is prepared.

A **new survey** of incident responders and hackers have some shocking statistics - (71%) can breach a targeted organization within 10 hours, and 18% claim they could breach a target in the hospitality and food and beverage industries within an hour. Paired with a miserable detection rate, these statistics should worry anyone in security and risk. However, system hardening and IDS/IPS systems proved to be effective. Most organizations are not taking the time to harden their systems – be sure that you are not left defenseless.

**GDPR** will be implemented in May, but its roll-out across the EU is not designed to provide a blank slate for businesses. Companies that have experienced a data breach, but have not reported it, have until the implementation date of May 25, 2018 to disclose the breach and notify users, or they could face significant penalties.

Finally, a new study has determined that **unpatched vulnerabilities** are the source of most data breaches. 60% of organizations that suffered a data breach in the past two years cite as the culprit a known vulnerability. Patching systems should be the first step any organization takes to ensure that their information systems and data are protected

~Stay Secure

*If you found this information valuable, we recommend taking a look at our weekly threat intelligence brief. For more information, contact us here.*

Bob Gaines
Director

646.375.9500 x114

rgaines@accumepartners.com

## Security Highlights

**IT Decision Makers Unsure about Their Security Maturity –** IT-decision makers in Asia Pacific, the United Kingdom, and the United States are only ‘moderately’ confident they are able to protect their organizations against hackers, and it might take time to find out when they have been breached. LogRhythm’s 2018 Cybersecurity Benchmark Survey polled 751 decision makers – of which less than half were able to detect a major cybersecurity incident within one hour. Even those who did detect a major incident would be unable to contain the breach within an hour. Source: https://securitybrief.com.au/story/it-decision-makers-unsure-about-their-security-maturity/

**Despite Risks, Nearly Half of IT Execs Don’t Rethink Cybersecurity After An Attack –** A wise person once said, "Insanity is doing the same thing over and over again and expecting different results." However, in a recent survey done by CyberArk for its Global Advanced Threat Landscape Report 2018 (registration required), almost half (46%) of 1,300 IT executives in seven countries say they rarely change their security strategy — even after a cyberattack. The survey findings suggest that a troubling degree of security inertia lurks within scores of organizations and effectively renders them unable to repel or contain cyber threats. Such complacency puts sensitive corporate data, IT infrastructure, and assets at risk. In fact, an overwhelming 46% of respondents say their organization can't stop the bad guys from infiltrating internal networks each time they try. Source: https://www.darkreading.com/vulnerabilities---threats/despite-risks-nearly-half-of-it-execs-dont-rethink-cybersecurity-after-an-attack/a/d-id/1331627

**Malaysia’s Central Bank Blocks Attempted SWIFT Fraud –** Malaysia's central bank says it detected and successfully blocked a Tuesday attack that attempted to steal funds via fraudulent SWIFT interbank money-moving messages. "All unauthorized transactions were stopped through prompt action in strong collaboration with SWIFT, other central banks and financial institutions," the country's Kuala Lumpur-based central bank, Bank Negara Malaysia, says in a statement. Brussels-based SWIFT is a global, member-owned cooperative that provides secure financial messaging services used by more than 11,000 financial institutions in more than 200 countries and territories around the world. SWIFT has been on the information security defensive since February 2016, when attackers stole $81 million from the central bank of Bangladesh's account at the New York Federal Reserve via fraudulent SWIFT messages, very nearly making off with $1 billion Source: https://www.bankinfosecurity.com/malaysias-central-bank-blocks-attempted-swift-fraud-a-10758

## Regulatory Headlines

**U.S. Regulator to Publish FinTech Charter Position in Next Few Months –** The head of the Office of the Comptroller of the Currency (OCC) said on Monday it will publish its position on a proposed charter for online lenders and other so-called fintech companies in the next three months. The fintech community has been watching closely to see if Joseph Otting, appointed U.S. Comptroller of the Currency in November, would push ahead with a charter to allow fintech firms to do business nationwide. “We haven’t concluded on the position and we welcome people’s feedback…” said Otting. Source: https://www.reuters.com/article/us-usa-occ-otting/u-s-regulator-to-publish-fintech-charter-position-in-next-few-months-idUSKBN1HG2FA

**New EU Fines Will Apply to ‘Old’ Data Breaches –** Companies operating in the EU that are currently hiding serious data breaches similar to those that rocked Facebook last month better disclose those before 25 May, or be prepared to pay serious fines. A European Commission official confirmed that data breaches that happened before 25 May, but are kept silent until after that, will be liable for fines. Source: https://euobserver.com/justice/141548

**PCI Security Standards Council: Activity Update –** As payment card fraud schemes evolve, the PCI Security Standards Council has to recalibrate its standards and programs with three key updates. Troy Leach, the council’s CTO describes three key updates: new PCI standards for software security and vendor lifecycle management, the update and expansion of the Qualified Integrator and Reseller training program, and moving the needle on validation and self-assessment for smaller enterprises with simplification. Source: https://www.bankinfosecurity.com/pci-security-standards-council-activity-update-a-10787

**IETF: GDPR Compliance Means Caring About What’s in Your Logfiles –** Sysadmins: while you're busy getting ready for the GDPR-regulated world, don't forget what your servers are storing in their logfiles. That advice comes courtesy of a draft mulled by the Internet Engineering Task Force's Internet Area Working Group (IETF's INTAREA). “In the past couple of years, new data privacy regulations with wide geographical scope are entering into effect with big effects for technology companies and technology consumers around the world. The combination of these changes, in IETF procedure and regulatory requirements, have caused some previously established best practices to become poor practices.” Source: https://www.theregister.co.uk/2018/04/24/ietf_gdpr_compliance_advice/

## Social Engineering

**Major Uptick in Mobile Phishing URL Click Rate –** In a study of Lookout users, more than half clicked mobile phishing URLs that bypassed existing security controls. Since 2011, Lookout has observed this mobile phishing URL click rate increase 85 percent year-over-year. “Mobile devices have eroded the corporate perimeter, limiting the effectiveness of traditional network security solutions like firewalls and secure web gateways,” said Aaron Cockerill, chief strategy officer at Lookout. “Operating outside the perimeter and freely accessing not just enterprise apps and SaaS, but also personal services like social media and email, mobile devices are rich targets for attack since they may lack enterprise security, but enable enterprise access and authentication.” Phishing attacks are particularly effective on mobile devices because hidden email headers and URLs make it easy to spoof email addresses and websites while new vectors, including SMS and messaging apps, enable attackers to make their campaigns personal. Source: https://www.helpnetsecurity.com/2018/04/10/mobile-phishing-2018-report/

**Mobile Phishing Threatens Enterprise Security –** The risk of phishing on mobile devices is growing, with more than half of mobile users clicking on compromised links in the last year. Phishing attacks are particularly effective on mobile devices because hidden email headers and URLs make it easy to spoof email addresses and websites while new vectors, including SMS and messaging apps, enable attackers to make their campaigns personal. “Attackers now take advantage of SMS, as well as some of today’s most popular and highly used social media apps and messaging platforms as a means of phishing,” says Aaron Cockerill, Chief Strategy Officer at Lookout. Source: http://it-online.co.za/2018/04/11/mobile-phishing-threatens-enterprise-security/

**GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Shipping Industry –** Unlike other BEC groups, GOLD GALLEON does not target a wide range of businesses but appears to focus solely on global maritime shipping businesses and their customers. CTU researchers estimate that between June 2017 and January 2018, GOLD GALLEON attempted to steal a minimum of $3.9 million U.S. dollars from maritime shipping businesses and their customers. The threat actors' theft attempts average $6.7 million per year. Source: https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry

**Cyber Crooks are More Interested in Exploiting People, Not Software Flaws, Claims Proofpoint –** Cyber criminals are increasingly attempting to exploit people rather than software flaws when launching devastating attacks, according to a new study. In 2017, the company analyzed attack attempts made on 6,000 organizations across the world. The report highlights the continued rise of ransomware, phishing, cryptocurrency threats and cloud application breaches. Source: https://www.computing.co.uk/ctg/news/3030362/ransomware-phishing-cryptocurrency-threats-and-cloud-attacks-are-growing-says-report

## Internal Threats

**Businesses Suspect Their Mobile Workers are Being Hacked –** More than half (57%) of organizations suspect their mobile workers have been hacked or caused a mobile security issue in the last 12 months, according to the iPass Mobile Security Report 2018. Overall, 81% of respondents said they had seen Wi-Fi related security incidents in the last 12 months, with cafés and coffee shops (62%) ranked as the venues where such incidents had occurred most. That was closely followed by airports (60%) and hotels (52%), with other locations on the list including train stations (30%), exhibition centers (26%), and in-flight (20%). Source: https://www.helpnetsecurity.com/2018/03/29/mobile-workers-hacked/

**Attacker Dwell Time Still Too Long, Research Shows –** New DBIR and M-Trends reports show the window between compromise and discovery are still way too long. In the past seven years, cybersecurity teams have cut down the time it takes to discover a security intrusion by fourfold. Unfortunately, that improvement in the window between initial attack and discovery of the incident isn't nearly enough to actually make a difference in blocking the typical intrusion from turning into a full-fledged data breach. Time to discovery is just the start of the journey in responding to a compromise. There's also the time it takes to respond to, contain, and investigate a threat. Source: https://www.darkreading.com/attacks-breaches/attacker-dwell-time-still-too-long-research-shows/d/d-id/1331519

**Companies Still Suffering From Poor Credential Hygiene: New Report –** A new report, the 2018 Privileged Access Threat Report from Bomgar, contains cause for worry for those who care about IT security since its numbers carry the clear message that, when it comes to keeping up with identities, most companies are getting it wrong. According to the survey of more than 1,000 IT professionals with ties to system access, half of companies polled say that they either have had a serious breach or expect one within the next six months. Of those giving a positive response to the breach question, roughly two-thirds pin the blame on misused credentials. Blame for this credential abuse falls on two large points: employee misuse, and misuse by trusted third parties. Source: https://www.darkreading.com/endpoint/authentication/companies-still-suffering-from-poor-credential-hygiene-new-report/d/d-id/1331554

**IT Must Patch Against Total Meltdown Now: The Source Code is on GitHub –** The source code for Total Meltdown, a vulnerability created when Microsoft tried to patch the initial Meltdown flaw, is now available on GitHub. A person known as XPN, whose blog lists them as a hacker and infosec researcher, posted detailsof a working exploit that takes advantage of Total Meltdown on Monday. In addition to that blog post, the source code for the exploit is now on GitHub, too. In the blog post, XPN describes Total Meltdown as a "pretty awesome" vulnerability in that it allows "any process to access and modify page table entries." XPN also noted that the goal was to create an exploit that could "elevate privileges during an assessment," but it was only to help other people understand the exploitation technique, not to create a read-to-use attack. Source: https://www.zdnet.com/article/it-must-patch-against-total-meltdown-now-the-source-code-is-on-github/

## Web/Internet Threats

**100% of Web Apps Contain Vulnerabilities –** A totality – a full 100% – of web applications are vulnerable to hackers. According to Trustwave's 2018 Global Security Report, derived from the analysis of billions of logged security and compromise events worldwide, all apps tested displayed at least 1 vulnerability, with 11 as the median number detected per application. A majority (85.9%) of web application vulnerabilities involved session management, allowing an attacker to eavesdrop on a user session to commandeer sensitive information. Source: https://www.infosecurity-magazine.com/news/100-of-web-apps-contain/

**Mirai Variant Botnet Takes Aim at Financials –** In January, a botnet based on Mirai was used to attack at least three European financial institutions. Criminals, like carpenters, hate to see a good tool go unused. It's no surprise, then, that the Mirai botnet has been in action once again, this time in concert with other botnets and with targets in the financial sector. Insikt Group, the threat research group within Recorded Future, found that a Mirai botnet variant was used to attack a company, or companies, in the financial sector in January. And it might not have been alone; they found that it was possibly linked to the IoTroop or Reaper botnet. Source: https://www.darkreading.com/attacks-breaches/mirai-variant-botnet-takes-aim-at-financials/d/d-id/1331472

**A Long-Awaited IoT Crisis is Here, and Many Devices Aren't Ready –** You know by now that Internet of Things devices like your router are often vulnerable to attack, the industry-wide lack of investment in security leaving the door open to a host of abuses. The content and web services firm Akamai published new findings that is has observed attackers actively exploiting a flaw in devices like routers and video game consoles that was originally exposed in 2006. Source: https://www.wired.com/story/upnp-router-game-console-vulnerabilities-exploited/

**Cyber Attackers Can Breach Targets in Hours, Report Reveals –** The majority of cyber attackers (71%) can breach a targeted organization within 10 hours, and 18% claim they could breach a target in the hospitality and food and beverage industries within an hour, according to the latest Nuix black report. Nearly 60% said it was rare for them to encounter systems that they could not break into, 75% of hackers said they were rarely detected by their victims after an attack and 2% said they were never detected. Some 74% said they were rarely impressed by an organisation's security posture and that most security professionals tasked with detecting attacks do not understand what they are looking for. Source: https://www.computerweekly.com/news/252439009/Cyber-attackers-can-breach-targets-in-hours-report-reveals

## Data Breaches

**SunTrust: 1.5 Million Clients' Details Potentially Stolen –** Great news: "SunTrust to offer free identity protection… at no cost on an ongoing basis." Indeed, the announcement of the supposed freebie comes by way of a press release from Atlanta-based SunTrust Banks, which some rank as being the country's fourteenth biggest bank. But the announcement comes with further red flags. The press release also announces: "SunTrust cares deeply about the privacy and security of client information." That, of course, is corporate-speak for a business that has lost control of its customers' data privacy and information security, potentially leading to fraud. Here's how: "[SunTrust] became aware of potential theft by a former employee of information from some of its contact lists," the release states. "Although the investigation is ongoing, SunTrust is proactively notifying approximately 1.5 million clients that certain information, such as name, address, phone number and certain account balances may have been exposed." Source: https://www.bankinfosecurity.com/blogs/suntrust-15-million-clients-details-potentially-stolen-p-2620

**Unpatched Vulnerabilities the Source of Most Data Breaches –** New studies show how patching continues to dog most organizations - with real consequences. Nearly 60% of organizations that suffered a data breach in the past two years cite as the culprit a known vulnerability for which they had not yet patched. Half of organizations in a new Ponemon Institute study conducted on behalf of ServiceNow say they were hit with one or more data breaches in the past two years, and 34% say they knew their systems were vulnerable prior to the attack. The study surveyed nearly 3,000 IT professionals worldwide on their patching practices. Patching software security flaws by now should seem like a no-brainer for organizations, yet most organizations still struggle to keep up with and manage the process of applying software updates. Source: https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465

**Hackers Once Stole a Casino's High-Roller Database Through a Thermometer in the Lobby Fish Tank –** Hackers are increasingly targeting "internet of things" devices to access corporate systems, using things like CCTV cameras or air-conditioning units, according to the CEO of a cybersecurity firm. Nicole Eagan, the CEO of Darktrace, told the WSJ CEO Council Conference in London on Thursday: "There's a lot of internet-of-things devices, everything from thermostats, refrigeration systems, HVAC systems, to people who bring in their Alexa devices into the offices. There's just a lot of IoT. It expands the attack surface, and most of this isn't covered by traditional defenses." Source: https://www.businessinsider.de/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?r=UK&IR=T

**Atlanta's Ransomware Cleanup Costs Hit $2.6 Million –** On March 22, a ransomware outbreak hit Atlanta city government systems, freezing not just the city's technology but also its ability to get work done. As a result of the outbreak, the city's 8,000 employees were unable to use their PCs for several days. The outbreak disrupted access to email, Oracle financial software, Siebel customer relationship management applications and Accela "civic engagement" software, as well as a Capricorn software self-service portal for residents, the city confirms. As a result, city residents were unable to pay for everything from water bills to parking tickets. City officials said they also ordered Atlanta's airport WiFi to be taken offline, "out of an abundance of caution." Source: https://www.govinfosecurity.com/atlantas-ransomware-cleanup-costs-hit-26-million-a-10888

## Threat Landscape

**New Figures Show Large Numbers of Businesses and Charities Suffer at Least One Cyber Attack in the Past Year –** With one month to go until new data protection laws come into force, UK businesses are being urged to protect themselves against cybercrime after new statistics show over four in ten (43%) of businesses and two in ten charities (19%) suffered a cyber breach or attack in the past 12 months. This figure rises to more than two thirds for large businesses, 72% of which identified a breach or attack. For the average large business the financial cost of all attacks over the past 12 months was £9,260 with some attacks costing significantly more. The most common breaches or attacks were via fraudulent emails - for example, attempting to coax staff into revealing passwords or financial information, or opening dangerous attachments - followed by instances of cyber criminals impersonating the organization online, then malware and viruses. Source: https://www.gov.uk/government/news/new-figures-show-large-numbers-of-businesses-and-charities-suffer-at-least-one-cyber-attack-in-the-past-year

**Cryptomining, Not Ransomware, the Top Malware Threat So Far This Year –** Cryptominer-based attacks, not ransomware-based attacks, have been the top threat so far this year, according to Comodo Cybersecurity Threat Research Labs' Q1 Global Malware Report. In the first three months of 2018, Comodo said it "detected 28.9 million cryptominer incidents out of a total of 300 million malware incidents, amounting to a 10 percent share. The number of unique cryptominer variants grew from 93,750 in January to 127,000 in March. At the same time, the data shows this criminal attention came at the expense of ransomware activity, with new variants falling from 124,320 in January to 71,540 in March, a 42 percent decrease." Source: https://www.csoonline.com/article/3269053/security/cryptomining-not-ransomware-the-top-malware-threat-so-far-this-year.html

**No Card Required: 'Black Box' ATM Attacks Move into Europe –** Fraudsters are now gingerly testing the waters in central and Western Europe with attacks that drain cash machines of their funds, according to a trade group that studies criminal activity around ATMs. The European Association for Secure Transactions, or EAST, says the attacks, sometimes referred to as "jackpotting," rose 231 percent in 2017 compared to 2016. Last year, 193 incidents were reported compared to 58 in 2016. Source: https://www.bankinfosecurity.com/no-card-required-black-box-atm-attacks-move-into-europe-a-10820

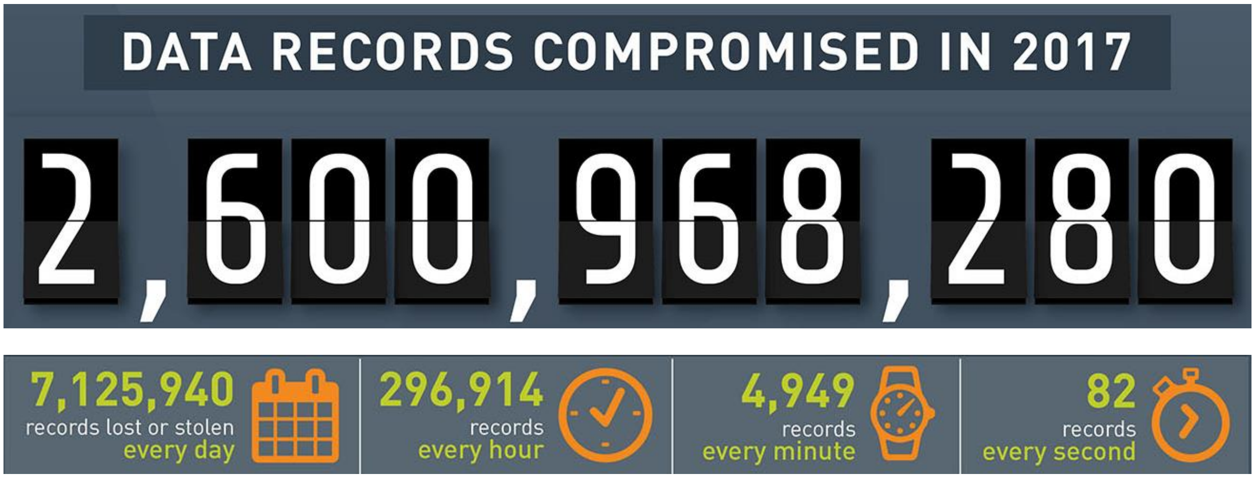
## Recommended Actions to take

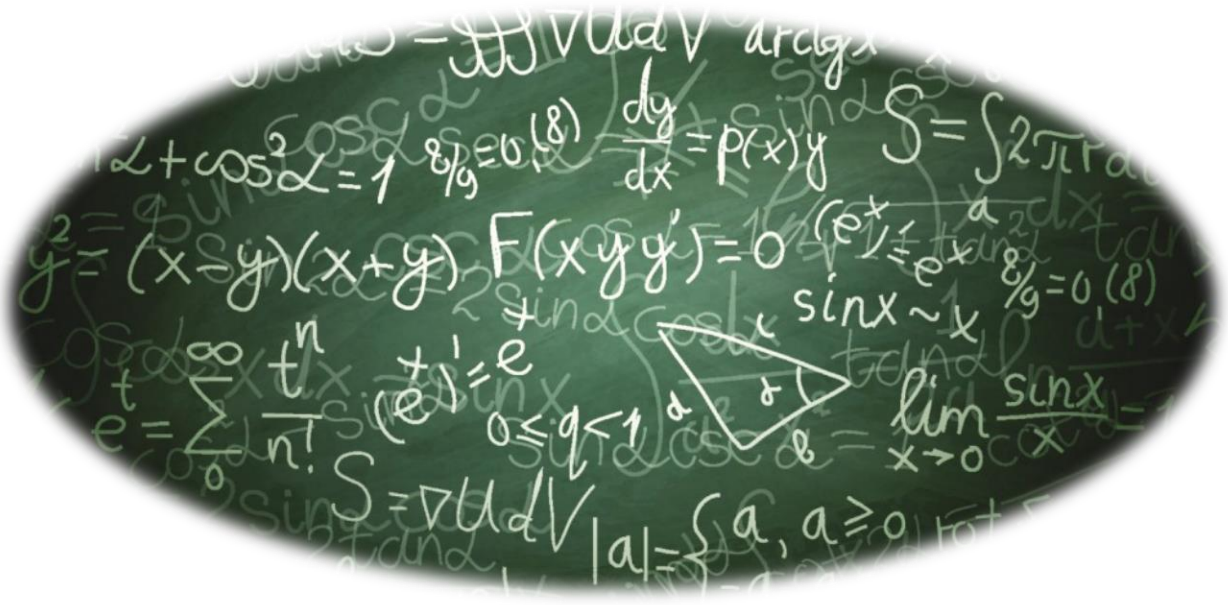
The following set of recommendations is based on the information provided above in the brief. For a more detailed set of recommendations, as well as vulnerabilities and indicators of compromise, please refer to Accume's weekly threat intelligence briefings.

- Ensure that your institution is aware of its requirements under GDPR and that it is taking the necessary steps for compliance if necessary.
- Ensure that your web filtering system can be dynamically updated against current threats
- Keep anti-virus systems up to date.
- Ensure that your security awareness program reviews phishing on mobile systems.
    1. Talk to your staff about phishing precautions they should take when reading email or text messages on their mobile devices
- Implement additional security controls for your mobile workers, such as VPNs and the use of portable hot-spots instead of utilizing public Wi-Fi
- Have your web page tested annually, and when major modifications to the code have been implemented
- Audit your firewalls, routers and switches annually
- Discuss the merits of hardening firewalls, routers, servers and workstations as an additional form of defense against attack
- Make sure that your incident response playbook is updated regularly to address the latest threats.

**If you have questions about any of the above recommendations, or about their implementation, feel free to reach out to Accume for additional information.**

*If you found this information valuable, we recommend our weekly threat intelligence brief, which has additional operational details for you and your staff. For more information, contact us here.*





*Considering the numbers, is your institution prepared to properly respond to security incidents? Accume can help!*