TORPEDO REPORT

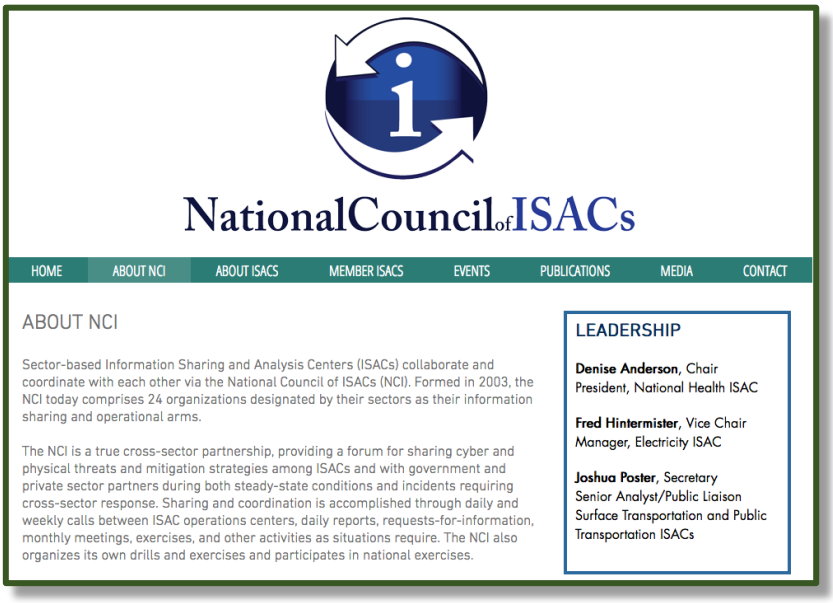
PUBLISHED:
11 AUG 2016
INFORMATION CUTOFF:
09 AUG 2016

IN THIS ISSUE…

HEALTHCARE CYBERSECURITY: HEALTHCARE TODAY, YOUR COMMUNITY TOMORROW

Summary. Banner Health, a Phoenix-based healthcare provider with facilities in seven states, recently announced that 3.7 million records they've kept on patients, doctors, and customers have been compromised by unknown hackers that gained access to their networks. Last month, the organization discovered that **malicious actors had been able to access the payment card processing systems used in food and beverage outlets in their hospitals**. Further investigation eventually revealed that the segment of the network that contained personal health information (PHI) on patients and health-insurance documents that contained information on doctors and providers. So far, this makes the breach potentially the worst healthcare leak in the state of Arizona since 2010.

Analysis. Exciting headlines have put a lot of focus on the healthcare sector of late, but the threats, challenges, and best practices for that vital community are largely applicable to almost any other organization – including critical infrastructure sectors, large, medium, and small businesses, non-profits, etc. The healthcare sector is finding itself increasingly targeted by hackers, in this case wanting to exfiltrate and monetize the valuable biometric and financial information that the sector holds on their patients and customers. This is on top of healthcare companies being an ideal victim for those criminals behind ransomware infections, as the loss of data could potentially lead to life-threatening complications for patients. However, ransomware and other easy attacks are not limited to the healthcare sector! Previous *Torpedo Reports* have already covered some considerations for organizations regarding ransomware and a threat-intelligence-based cybersecurity policy, which are just as applicable to the healthcare sector as any other. To its benefit, the healthcare sector has the National Health Information Sharing and Analysis Center (NH-ISAC), which is a powerful tool for organizations under attack to become part of a community dedicated to sharing information and finding solutions to prominent security problems. Other sectors also have ISACs and Information Sharing and Analysis Organizations for their communities (if you are unsure where to start, check out the National Council of ISACs website or contact our team and we'll be glad to help point you in the right direction).



Preparedness & Operational Considerations.

1. **Planning**. A key service of an ISAC is to provide critical infrastructure sectors with the sort of actionable intelligence leaders need to make educated decisions. Whether through information sharing portals, collaborative lists, or other arrangements, ISACs can harness industry specific analysis to contextualize member-provided, open-source, for-cost services and public-sector-provided threat news. For example, NH-ISAC offers CYBERFIT™, a mixture of cybersecurity services,

__The Torpedo Report__ is a weekly report produced by Gate 15. Torpedo is a modified acronym for Threat, Risk, Preparedness and Operations. The Torpedo Report is intended to provide an assessment of key notable threats highlighted over the previous week with operational context, risk analysis and actionable preparedness and operational recommendations leaders can consider to enhance their organizational security and resilience.

including threat intelligence, all tailored to the healthcare sector. Other sectors have other resources and tools available to facilities timely information exchange and security awareness (for more information on ISACs generally, read this brief summary from the National Council of ISACs website). ISACs can help members develop a sound understanding of the threat environment and the communities' relevant risks, allowing leaders a trusted community to discuss how to manage their organizational risks and concerns.

2. **Training**. ISACs can provide your employees with access to training and discussions with peers that cover contemporary, pressing topics to the industry at large. For example, NH-ISAC hosts multiple Medical Device Security Workshops, where invited experts and key personnel can talk through the implications of internet-connected healthcare devices, their cybersecurity vulnerabilities, and what the sector can do to mitigate the risks to patients. The NH-ISAC, in coordination with FS-ISAC, MS-ISAC, government partners and service providers, are also conducting a series of Nationwide Ransomware Roadshows to educate small and medium size businesses. This sort of community exchange, using resources from across a wide spectrum of disciplines and making it applicable and collaborative for a specific community, is only possible through an ISAC or similar organization capable of taking a sector-wide / community-wide view of the threat environment, being able to understand and process the relevant risks, and helping community members identify their greatest concerns.
3. **Exercise**. Many ISACs have participated in a variety of exercises with their members and with government. From high-level national exercise events validating the information sharing and collaborative processes between industry and government to sector-specific drills exercising intra-ISAC processes and procedures to ensure readiness to respond to major threats and events, ISACs help members develop and test their ability to react to the dynamic threat environment. Some ISACs can also provide resources or contacts to help members conduct their own exercises ensuring robust preparedness from member to ISAC to government and the cross-sector community.
4. **Operations**. Membership in an ISAC should have an effect on your organization's day-to-day operations and processes and procedures will need to be created in response. These should address how to internally capture the types of threat information, suspicious activities, and indicators of compromise your company is comfortable sharing (anonymously if desired) with the ISAC and other members, as well as to take advantage of the intelligence that's made available from ISAC analysts and via automated intelligence tools.

BUSINESS CONTINUITY: YOU PLAY LIKE YOU PRACTICE

Summary. On Monday, a system outage at Delta's Atlanta-based command center resulted in the cancellation of 450 flights and delays affecting thousands more across the airline's global network. The aftereffects of the outage - which took offline almost every device that Delta uses to track planes, crew, passengers, weather, and maintenance - lasted for more than 24 hours, with over 250 cancellations necessary the next day and residual impacts still continuing. While Delta has not released the full details behind the glitch, it's being reported that, around 2:30 AM local time, there was a power outage at the facility. What's currently unknown is why Delta's contingency measures for such an occasion failed, leaving critical machines unable to transmit information.

Analysis. At this time, it doesn't appear that Delta's difficulties are related to malicious activity but rather a far more common enemy – the reality that inevitably something will go awry. While Delta had a backup command center and power generator in place, it appears that they did not test the transfer process rigorously enough to discover the mistake that undid them on Monday. Alternatively, it's possible that Delta had recently changed a component necessary for that transfer of power, leading to failure in a real world situation. One adage that has remained consistent as infrastructure ages and technology advances is that, unfortunately, "$h!t happens." In our fast –paced economy, organizations cannot afford downtime – neither financially nor from concerns around reputational risk (take a look at #delta, #DeltaSucks, or other variations on social media to peek into some of Delta's resulting social media grief). Operational and equipment redundancy are and will always remain vital. However, redundancy without proper preparedness is unlikely to be effective.

Preparedness & Operational Considerations.

1. **Planning**. Organizations need to have established protocols for how to respond to the various incidents and disruptions they may face. Some of these will be high-level plans for senior leaders and some will need to be quick response checklist-type references for what to do when something breaks. While many organizations rely on institutional knowledge, over-reliance on individuals vs. processes can lead to significant failures (especially since things always seem to go wrong at 2:30 am… in the rain… when someone's sick). Organizational maturity requires established plans, procedures, and protocols for all levels.
2. **Training**. Plans are a good start, but then personnel need to be familiarized with their specific roles and responsibilities and to have regular opportunities to practice responding critical tasks. Whether power outages, restoring from back-up after a ransomware attack, or relocating and operating from alternate facilities after a hurricane or terrorist attack renders primary locations unavailable, personnel need to be trained on vital, perishable skills. As football season ramps up, veteran players still return for OTAs to start getting ready for game time. Your key players also need to have opportunities to pause, meet with their teammates and go over the X's and O's.

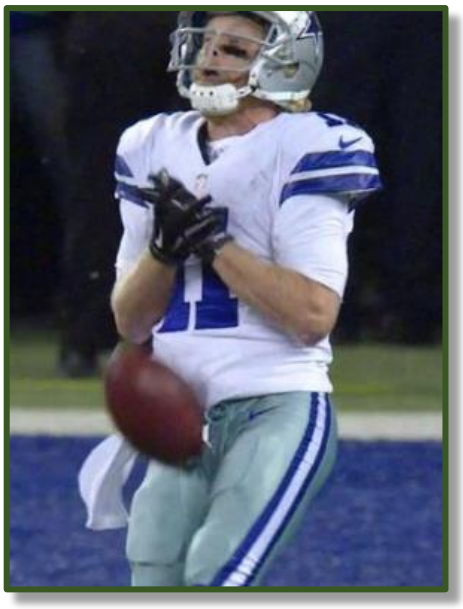


FIGURE 1: Whoops. Photo via SB Nation

3. **Exercise**. As demonstrated in this instance, having a back-up data center and redundant systems available for vital assets is an important step for resilience and preparedness. However, they mean nothing if your personnel are unable to execute the transfer process during a real emergency, whether it's due to lack of training or faulty equipment. Consider how often your organization exercises contingency and continuity plans related to vital assets and core functions. Does this happen often enough to stress test and educate employees on any modifications to the hardware involved in the process? Could your employees execute the transfer with minimal insight from reference documents? If a data center is valuable enough to your company's bottom line, frequently setting aside the time for employees to train on recovery operations is extremely valuable to maximizing uptime. Continuing the football metaphor, after OTAs, preseason games allow the team to work out the kinks, practice the plays and learn how to execute correctly before the regular season begins. Exercises are preseason football. Your starters need to be in the mix, and so do the back-ups. Train and exercise all 53 team members and you have depth and redundancy. Train your starting twenty-two, or just the bench, and you're begging for big time fumbles in critical situations.