Success Stories in Cybersecurity Information Sharing

BY DAVID S. TURETSKY, BRIAN H. NUSSBAUM AND UNAL TATAR

JULY 2020
Cybersecurity — protecting our digital systems and the confidentiality, integrity and availability of information that is on and transiting them — is an endless challenge. Like many other challenges, coordinated and collective responses are often more effective than individual or conflicting ones. Information sharing is about precisely that.

\footnote{College of Emergency Preparedness, Homeland Security and Cybersecurity ("CEHC") at the University at Albany–State University of New York. All three authors are on the faculty of CEHC: David Turetsky is Professor of Practice and Brian Nussbaum and Unal Tatar are Assistant Professors. The authors would like to acknowledge and thank the William and Flora Hewlett Foundation for its support of this project.}
INTRODUCTION

The more useful and up-to-date information we have about what attackers are doing — their motivations, targets, and attacks, and the tactics, techniques and procedures they favor — the better the chance of stopping them. Developing useful information quickly and more comprehensively, and sharing it immediately in an actionable form with potential targets, improves their ability to take action promptly. Such action can include identifying threats, patching or otherwise reducing potential vulnerabilities, and ultimately avoiding harm from the attacker. From an economic perspective, information sharing can help to lower the cost of defense; by helping defenders to understand exactly which threats are prevalent, what to look for and prioritize, and how to defend effectively against these threats. It can also raise the cost to attackers. The tools attackers use can require considerable time, resources and expertise to develop. Information sharing can shorten the time, and reduce the instances, in which those tools can generate substantial spoils through re-use. That means that attackers may need to invest more in hacking tools to generate the returns they could earn if there is not effective information sharing, which also increases deterrence by denial (Denning 2015). Thus, information sharing both allows defense to scale, and precludes some attacks from being able to scale; helping to even the playing field between defense and offense.

The theory behind information sharing seems uncontroversial. It is largely analogous to our efforts to combat crime or spying. We try to develop information on the practices of criminals or spies, including knowledge and understanding of their crimes and of the patterns of their activity. We then use that information to try to catch or stop them, and make it harder for them to succeed. The concept of a neighborhood watch also embodies this theory, where actual or potential victim-stakeholders organize to observe, gather and share information to make it less likely that they will be successfully attacked individually, or collectively, by the same actor or through the same tactics, techniques and procedures. Better situational awareness leads to better and more successful risk management. Putting information from multiple sources together to do a job better is what cybersecurity information sharing is about. This echoes our broader era as well, with big data and machine learning increasingly providing greater insight into, and sometimes guiding, activities of all kinds. Information sharing across organizations is one way in which cybersecurity is becoming more data and evidence based—relying not just on the experiences of one organization, but based on the data and experiences across sectors and industries.

WHY FOCUS ON STUDYING “SUCCESS STORIES”?

What seems clear in theory, should be visible in practice. If the benefits of cybersecurity information sharing in theory are obvious, then it should be possible to identify real world experiences that reflect those benefits, including circumstances where information sharing participants have avoided harm due to shared information. The absence of success stories would not necessarily mean there was no benefit to information sharing, but it would be a disconcerting data point. That said, that is not a problem, because it turns out there are many success stories to be collected and assessed.

This documentation is important because most companies do not yet engage in formal information sharing, and the question of whether to do so, broadly speaking, arises frequently. Sometimes what weighs on the benefits side of the scale when companies or other organizations consider whether to participate in information sharing is somewhat less well understood and harder to value — more speculative and less tangible — than what lies on the cost or liability side of the scale. First,
many C-suite executives or boards perceive and weigh various risks from engaging in information sharing, such as to reputation, but may have seen or understood fewer tangible examples of the benefits, including the harm that might be avoided. If the risks are clearer than the benefits, that may contribute to companies or other organizations being less willing to support and prioritize information sharing than should happen. Second, effective information sharing requires the commitment of resources, and that means it is important to understand not only the costs, but also the benefits of the expenditures. Sharing mechanisms, especially automated ones that allow current information to be shared quickly, require commitments of technology, people and resources that could be used to pursue other opportunities. Investment in these “hard costs” is required to make information sharing work effectively and for shared information to be “actionable.” Third, there are few very well-accepted and widely used metrics to quantify the real-world benefits of information sharing. While some exist, they tend to focus on quantity over quality, the latter obviously being tougher to measure. Throughout the field of cybersecurity, whether the issue is the effectiveness of particular practices or tools, or of the importance of aspects like supply chain, “metrics” has been a topic of thought, discussion and debate. In the absence of widely-used and accepted metrics, it is important to provide other credible and understandable evidence that can help to educate or influence C-Suite and Board members who often may not be very technically-oriented.

The idea for this project stemmed from one of our authors’ work on information sharing issues for years in several different contexts, including in the public and private sectors and academia. It was clear that the absence of a cross-sectoral collection of information sharing success stories was a gap. Even some victims that had been hacked by a well-known attacker opted against engaging in formal information sharing, concerned about the potential risks, and less certain of the benefits. Neither passage and implementation of the Cybersecurity Information Sharing Act of 2015, nor the written work of the Information Sharing and Analysis Organization (ISAO) Standards Organization filled this gap.

**WHAT IS THIS PROJECT?**

This project had two principal elements. The first was to bring together some of the leaders in the cybersecurity information sharing field to discuss information sharing success stories; to focus on successes, generate information or evidence, and to highlight the need for and value of documentation of successes. The second was to disseminate such stories and evidence more widely, to pull together a range of information sharing success stories across different sectors, including not only multiple industries, but also successes in state or local government and academia.

There could be many different ways to focus on information sharing successes. We chose to focus on what we call success stories, instances where it appears that as a result of shared information, there was a high likelihood or certainty that a recipient avoided or reduced harm. We thought this relatively straightforward approach could produce a helpful product that could be understood easily by people who were not necessarily technically adept and engaged in computer security, but who might be involved in decision making about information sharing or cyber risk management. We thought that it could be a launching point for future work, additional collaborations, and other attention that would further develop and hone the benefits of information sharing, and perhaps increase its adoption.

We targeted three main audiences for this project. First, we sought to produce something that might be informative to the process by which companies or other organizations make decisions about whether to participate in information sharing organizations or programs. Second, we hoped that the product might be useful in two ways to information sharing organizations, such as ISAOs and Information Sharing and Analysis Centers (ISACs), to help them describe the concrete benefits of participation to prospective and possibly even current members, and to increase their focus on the collection of success stories and other evidence of success. We thought both of these could help them in a number of ways, to assist in their efforts to expand participation and, potentially, to use any enhanced understanding of these successes to help in their continuous efforts to improve their work for members. We also thought that this could supplement their more easily observed metric of success, the extent to which their membership was increasing.

Third, we recognized that policy makers have devoted attention and effort to promote information sharing and we hoped that the product might be a useful resource for them, and perhaps help confirm that their past and continued efforts to promote it are beneficial. Information sharing is not a panacea, and will not fix cybersecurity challenges writ large. It is, however, an important and powerful tool, and one where the advantages and successes have not been well documented in any systematic way.
As part of this project, we interviewed — by telephone or in person — a substantial number of individuals who have been involved with information sharing across many sectors and industries. Our interviews were primarily with those who work, or recently worked, at an ISAC or ISAO, or in a company or other organization that takes part in information sharing programs or organizations. Information sharing operates on trust, and we understood that. As a result, we often agreed when we spoke with individual entities about specific cases, not to identify those entities by name, but rather by sector, size, or similar characteristics.

In October, 2018, we held a conference on cybersecurity information sharing in Albany, New York, on the campus of the University at Albany, part of the State University of New York. The conference was co-sponsored with the University by the MS-ISAC (Multi-State Information Sharing and Analysis Center), based in East Greenbush, NY, just a few miles from the University. To promote frank conversation and more sharing of experiences, the morning session of the conference was not open to the public. It included under 30 people. The participants included national leaders of various ISACs or ISAOs in a range of sectors, such as IT, health, financial, telecommunications, electric, state and local government, and academia. Some sectors had multiple representatives present. The authors moderated the discussion. A small number of CISOs (Chief Information Security Officers), or other cybersecurity leaders, from the local area attended, as did academic colleagues, including from the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany, where the authors are on faculty, but also from other University units covering business, education and public health, along with Albany Law School. A few undergraduate and graduate students involved with the project in some fashion attended as well.

The afternoon sessions moved to a larger venue on campus and were open to the public. The afternoon consisted of a number of opening remarks, by the Provost of the University, by the Dean of the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany, where the authors are on faculty, but also from other University units covering business, education and public health, along with Albany Law School. A few undergraduate and graduate students involved with the project in some fashion attended as well.

The authors moderated the discussion. A small number of CISOs (Chief Information Security Officers), or other cybersecurity leaders, from the local area attended, as did academic colleagues, including from the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany, where the authors are on faculty, but also from other University units covering business, education and public health, along with Albany Law School. A few undergraduate and graduate students involved with the project in some fashion attended as well.

There are even some initial attempts to measure or assess the effectiveness and “success” of information sharing schemes, however these are far from mature or complete. Much of this work refers to types of benefits. Notably, there is a strong emphasis on measurement and metrics (Fleming 2012) which — while important — can vary in terms of organizational applicability and utility, including the extent to which it signifies a

**LITERATURE**

**Studying Information Sharing: Modeling, Measurement, and Telling Stories**

This project is hardly the first time that some aspect of information sharing in the context of cybersecurity has been studied. There is literature attempting to define information sharing and its constituent parts, and suggesting principles (Fisk 2015), frameworks (Johnson et al. 2015, Vazquez et al. 2012), and technical processes for sharing (Barnum 2012). There are attempts to model information sharing and the decisions involved using concepts from game theory (Tosh et al. 2015) to public health (Sedenburg et al. 2015). There are examinations of the tradeoffs, risks (Bhatia et al. 2016), privacy costs (Heidenreich 2015), and potential organizational downsides to information sharing (Gordon et al. 2015). There are industrial case studies ranging from finance (Hausken 2005) to national security (Jasper 2017) to critical infrastructure owners and operators (Fleming 2012). There are economic analyses of the incentives to share (Gal-or and Ghose 2005) and the consequences of sharing (Gal-or and Ghose 2004).

There are even some initial attempts to measure or assess the effectiveness and “success” of information sharing schemes, however these are far from mature or complete. Much of this work refers to types of benefits. Notably, there is a strong emphasis on measurement and metrics (Fleming 2012) which — while important — can vary in terms of organizational applicability and utility, including the extent to which it signifies a

---

1. Our interviews extended beyond those who attended the conference to representatives of many more sectors, such as retail, transportation, natural resources, technology and others.
2. Of these, the authors would particularly like to thank and acknowledge our small team of research assistants throughout this project, Meghan Anderson, Manpreet Duggal, and Jesse Parent. We are grateful for their assistance with and participation in interviews, organizing and making the conference successful, organizing the information generated through this project, and for their helpful ideas and insights. This paper reflects their contribution as well as ours.
success that results in avoiding harm. One can, for example, count the number of information sharing alerts or products, the number of each type of information shared, the numbers of IP addresses blocked, etc. This project is designed to supplement the existing literatures, by offering some important qualitative — and narrative — balance to these models and metrics.

According to the management (Weick and Browning 1986) and organizational studies (Van de Ven and Poole 2005) literatures, narrative approaches often offer important abilities to catalyze change and provide insight. That is, success stories like the ones presented here are an important component of effectively communicating the value of information sharing, its ability to benefit individual organizations as well as to improve the broader ecosystem of particular industrial sectors. That is, a story about a financial institution benefiting from information sharing is a win both for that organization and also for the broader financial services sector. Narratives, particularly success stories like these, are an important component of documenting these micro and macro improvements in cybersecurity.

**SUMMARY**

We found that there is indeed persuasive evidence, in the form of success stories, to demonstrate that information sharing has been successful across the U.S. economy and amongst various sectors — from non-profit organizations, to companies, to academia, and including state and local for-profit government. While the evidence we collected is anecdotal in a sense, it is collectively powerful and persuasive nonetheless, particularly when coupled with the strong theoretical underpinnings of information sharing.

While any one success story could certainly be a result of industry context, the individuals involved, a particular organizational culture or some other variable, when we begin to see successes across industries, across organization types, and across time, it begins to look like these success stories are not just stand alone tales, but rather part of a broader process of improving the cybersecurity environment. We saw examples of success stories that reflected that the benefits of information sharing can be delivered by a variety of means.

**Industry Level Sharing**

Many success stories involved sharing by entities in the same industry through ISAOs or ISACs organized by industry. They enhanced the ability of targets to take steps to avoid or mitigate harm, more quickly informing them of what to look for and how to avoid harm. Information sharing extended the time for targets to prepare and sometimes that made all the difference.

**Multiple Sharing Platforms or Organizations**

Some entities were members of multiple information sharing organizations. One example is a company that is a member of both retail sector and financial services sharing organizations, since as a large retailer the company handled a substantial volume of credit card and other payments in addition to its core retail function. This proved important, because not every sectoral information sharing organization focuses on the same threats.

**Formal and Informal Sharing Organizations**

Some of the entities that shared through a sectoral ISAC or ISAO, also shared through a smaller and sometimes less formal group of peers in the same industry, where there were even stronger bonds of trust. This additional sharing built upon the sharing through the organizations of which they were each a part. While ISACs and ISAOs formalize information sharing processes, it is important not to discount sharing that happens informally — even though it is harder to track or measure.

**Company and Government Sharing Relationships**

Some entities shared information with (including receiving threat information directly from) the federal government. Sometimes they received or shared information directly, whether it was in written form such as an alert, or orally as in dialogue with the FBI. Sometimes the engagement was indirect, as when they sought or provided information from or to the government through an ISAC. This mix of ISAC/ISAO mediated sharing and direct firm to agency sharing is worth acknowledging — sometimes sharing organizations offer an important buffer for organizations, whereas other times direct interaction with law enforcement or the intelligence community is preferable. Whether the organization shared directly or indirectly with the government, and sometimes the preference of an organization was not to identify itself and share directly with the government, they believe they obtained important benefits from sharing information with the government.

**Defining Success**

The success stories demonstrate that success comes in many types. Often, an entity was able to spot threats quickly, some of which had already penetrated its perimeter, because of information it received. It would not likely have been able to do so without information sharing. Other times, it quickly learned what it should patch or update to reduce vulnerability. Still other times, information sharing enabled industry to identify
broader vulnerabilities and problems and act together. Organizations were able to spot supply chain risks that they had not previously seen, or could not have seen or understood themselves without an ISAC/ISAO aggregating information from across their sector. Some ISACs also served as forums or catalysts, and not only provided benefit directly to members, but also served as launch points for members to share information and network with others less formally. Moving forward, it is important to treat each of these as potential varieties of success in information sharing.

Below, we provide examples of success stories from our research. We provide the first few stories in greater detail. Then we briefly summarize some others grouped by economic sector.

SUCCESS STORIES

1. Information Sharing Enables a Financial Services Company, and Similar Companies, to Identify Threat from Hidden Cobra, North Korea

This story involves multiple instances of information sharing by a financial services company, involving at various times the government, other financial services companies, and an information sharing organization, FS (Financial Services)-ISAC. Because of what was learned through these instances of information sharing, the financial services company and other financial services companies were able to identify, and sidestep, adversarial cyber threats from North Korea that were part of a program by what is referred to as “Hidden Cobra.”

The U.S. government published an alert in June, 2017, which was updated in August, 2017, DHS/FBI TA17-164A. Id. This alert shared information about cyber threats from Hidden Cobra, which is associated with North Korea, including certain IP addresses. Much later, in March, 2018 and again from June through August, the financial services company detected suspected scanning activity from an IP address that was associated with Hidden Cobra actors, according to the alert from the better part of a year earlier.

Seeing this activity, the financial services company was concerned because it recognized the IP address and understood that malicious cyber activity often commences with an adversary conducting scanning and reconnaissance against its target. Often, this reflects efforts by an adversary to map its infrastructure, detect vulnerabilities, and map ways to exploit the target. The “Kill Chain,” a major cyber defensive framework (Hutchins, Cloppert, Amin, 2011), focuses on spotting and stopping adverse conduct at various stages, including at the reconnaissance stage that initiates that Kill Chain.

After seeing this activity, the financial services company reached out to other financial services companies, noting what it had seen and asking whether any of them had seen similar behavior involving that IP address. The company learned that multiple other financial services companies had also seen similar scanning and activity.

The financial services company also reached out to FS-ISAC, an information sharing organization of which it is a member. The company wanted FS-ISAC to submit requests for information to the U.S. government, to DHS and the FBI, the entities that had issued the Alert, to learn whether the relevant IP addresses were still a part of the Hidden Cobra infrastructure. The U.S. government responded that the IP addresses should still be considered part of the Hidden Cobra infrastructure.

With the information learned from the original U.S. Government Alert, the information shared with and received from other financial services companies, and the information shared with and received from the U.S. Government through FS-ISAC, the financial services company took action and dropped all of the packets and no compromise occurred. Not only was the financial services company protected, but the sharing in which it engaged also enabled other financial services companies to identify and defend against malicious activity. This combination of financial service company peer-to-peer information sharing and mediated sharing between financial services companies and the intelligence community, demonstrates effective sharing within the private sector, as well as between the private and public sector.

---

The information sharing experience of this financial services company in connection with this story is reflected in this exhibit:

2. Cozy Bear and a Financial Institution

Another success story of a financial institution’s engagement in information sharing reflected the use of some information it originally obtained from a vetted community forum, and later supplemented with information sharing through the FSARC (Financial Systemic Analysis & Resilience Center) listserv. FSARC is an information sharing membership organization comprised of large financial institutions. This information helped the institution to recognize, identify, and investigate an illicit email targeting it — and to avoid potential harm. The information also enabled the institution to understand better and prioritize certain threats, threat actors and their motivations, going forward.

This story began in 2016, when a cyber threat analysis team member from the financial institution explored a link that was posted on a community forum to a blog post written by a security firm. The blog post discussed cyber threat activities by Cozy Bear, Russian cyber actors, and noted certain malicious email formats that had been used by those actors. Following up, the team determined that an individual at their institution had received a similar email. The targeted individual had significant political connections, and information about that individual’s connections was publicly accessible on social media. The email came just two days after the 2016 election. It was a spear-phishing attempt from a compromised email account at a leading prestigious university. The user did not open the email before it was discovered.

In addition, through information sharing about the incident on the FSARC listserv, the financial institution was able to determine that two other institutions also...
were targeted. As a result, all of those who followed the FSARC listserv became aware of the danger and of the targeting of their sector. Because Cozy Bear actors had not previously been known to target financial institutions, that information was particularly significant. The information not only helped multiple institutions with respect to the specific conduct that was identified, but was also important to the financial institution in this case and likely to others, for prioritizing analysis of Cozy Bear actors (and similar political and espionage actors), and for understanding their targeting methods and assessing their motivations for targeting the financial sector. This sharing by private sector security firms with the financial sector, and among systemically important financial sector members, led to a significant updating of the sector’s cyber threat assessment model, and enabled threats that would have caused harm to be identified, understood and addressed.

3. MS-ISAC Sophisticated Airport Infection Case*

The MS-ISAC received “a note” from the National Cybersecurity and Communications Integration Center (NCCIC) in the national capital region asking whether the MS-ISAC — which was then monitoring network traffic for about one third of U.S. states — had seen any activity from a particular IP address. The MS-ISAC began to look through their logs and records, and discovered communication between that IP address and a computer in one of the states for which they monitored traffic. They reached out to that state to inquire what the computer was, and to get further information. The state replied that this particular computer was an email server at an airport. MS-ISAC, wanting to investigate further, requested a copy of the email communication. The state shared the email with MS-ISAC.

It was a phishing email that had gone to someone at the airport describing an industry conference. The email, it turns out, had gone to about a dozen different airport executives. MS-ISAC continued its investigation by examining the names of the dozen airport executives who had received the email. When they began using an online search engine to investigate, it quickly became clear that all of the airport officials had their names and contact information listed on a single online document. The online document was a .pdf file listing all the airport contacts. MS-ISAC did further research, and ultimately reached out to the industry association that had posted the .pdf file listing all the airport contacts.

MS-ISAC then sent out an advisory to states and cities — their main clientele — with details and indicators in case anyone else had seen similar traffic. Had this story ended here, it would have been an information sharing success story. But there was more to come. One city responded to MS-ISAC that they had seen similar traffic. MS-ISAC was actually able to do forensic examinations of the city’s airport computers to find out what had happened.

According to their forensic analysis, the attacker had leveraged this email and the associated malware to get “…access to security cameras and the ticketing terminals.” This is a hugely consequential malware infection, and had apparently been targeted at everyone on the list of airport contacts from the industry association. MS-ISAC did further research, and ultimately reached out again to the industry association that had posted the .pdf file listing all the airport contacts.

MS-ISAC asked the industry association whether they kept logs for the website, including the piece of it that hosted the contact list. They did. The MS-ISAC asked for records about any downloads of that list during the period prior to the phishing emails being sent. According to the MS-ISAC, “There was one download.” The industry group provided information on the associated IP address to MS-ISAC, and the ISAC was able to establish that it was an IP address “…that was known to do reconnaissance for nation-state type attacks associated with China.”

With this information, MS-ISAC quickly contacted federal partners — including TSA and other DHS components — to brief them on the results of their investigations. To avoid harm, TSA subsequently sent notices to airports in the United States. This is a clear success story where initial sharing about a single potentially malicious IP address lead to a successful investigation, forensic work, and further information sharing that crossed levels of government and the public and private sectors.

4. MS-ISAC Streaming Video Supply Chain Case*

This case began with a federal entity, the DHS, reaching out to the MS-ISAC with a question about activity to a particular IP address based in Estonia. When MS-ISAC began looking through its logs and records, they discovered that “lots of states” were “beaconing” out to this IP address in Estonia every two hours. In each case, the device beaconing out was a streaming video appliance.

With that, the MS-ISAC began its investigation. By looking through their data, they discovered numerous states
and cities that had similar beaconing activity, all coming from streaming video devices from one manufacturer. There was an interesting reason that MS-ISAC had unique insight into this problem. “These devices were very, very, popular with state and local government, these devices were broadcasting town hall meetings, state legislative hearings, senate hearings, but these devices were also connected into the networks.”

MS-ISAC reached out to this manufacturer and described the activity involved. Initially, the manufacturer said, “This can’t be happening,” and was convinced that they did not have a vulnerability. “What they discovered was, in the build process, some of the component pieces in the supply chain added a little bit of code to the streaming video devices.” The company issued an alert to affected customers and “patched and updated their servers.” At this point, the problem had — assumedly — been solved.

However, a week later, MS-ISAC checked its logs again and, sure enough, there was beaconing activity to the Estonian IP address. MS-ISAC reached out to the manufacturer, who assured the ISAC that they had identified the “batches” of devices where problematic code could be, and patched them all. The MS-ISAC and manufacturer shared additional information back and forth, and it became clear that the manufacturer had “underestimated the number of batches that were compromised.” The devices were subsequently patched and made secure.

This case was an interesting success story for several reasons. First, while the movement of information from DHS to an ISAC to its customers is not necessarily unusual, the involvement of the manufacturer, and particularly patches that eliminate the problem is more unusual. Secondly, this was one of the first cases that MS-ISAC had seen involving compromises of supply chains, something that has become a high profile concern in recent years.

### 5. Iran steals intellectual property from universities

In March, 2018, the U.S. Department of Justice revealed an indictment against nine Iranians working on behalf of the Islamic Revolutionary Guard Corps to target intellectual property and data in a hacking campaign affecting the accounts of thousands of professors at hundreds of universities around the world. In addition to professors, the targets included academic publishers and repositories of academic articles and information, a biotech company and several technology companies. The indictment referred to “massive, coordinated cyber intrusions into computer systems belonging to at least approximately 144 United states-based universities...” and a slightly larger number of universities in other countries around the world.

It all could have been much worse. Through information sharing before the public was made aware of what was happening, numerous academic institutions were already alerted to the problem, the tactics, techniques, and procedures of the attackers, and their objectives. After a few academic institutions had fallen victim to these attacks, some of these institutions shared information about the malicious acts against them through REN-ISAC (the Research and Education Networks Information Sharing and Analysis Center). The results were unexpected. Several additional institutions responded by saying they too were experiencing similar attacks. This alerted the sector that comparable attacks were occurring on a scale and level of sophistication not seen before, and to the objectives of these attacks. It enabled the sector to interpret the activity in the proper context and thereby focus more effectively and prioritize detection, preparation, defense and response.

The experience of one large U.S. academic institution illustrates the value of the information sharing. In August, 2016, its faculty began to forward and report targeted phishing messages purporting to be from colleagues in the same field based at Canadian universities. The messages appeared to be signed by real faculty working in their disciplines, but were sent from lookalike or “typosquatted” domains, e.g., umontreall.ca and uturunto.ca. The link in the spear phishing email pointed to a replica of the library’s periodical log-in page. This false page was likely the means to gather log-in credentials of faculty. The university took action but also shared the information with its peers through REN-ISAC. Several other schools reported receiving similar phishing emails. Over the next year, the institution engaged with the FBI, and shared and received information. It also experienced numerous additional attempts to connect to various scholarly articles with stolen faculty credentials, often involving log-in attempts via the campus’ VPN from a proxy server in Germany. Additional steps were taken to block this activity and information about these additional attacks was

---

shared with peers through REN-ISAC. In the exchanges through REN-ISAC, the institution learned that Iranian actors were suspected of being behind the attacks, and that one of the purposes was to gain access to periodical indexes and scholarly journals, or sell access to those resources by marketing stolen university credentials, as evidenced by the VPN activity from Germany. The academic institution believes that the information it shared helped other universities better understand the attacks and avoid harm, and found the information it received through REN-ISAC from other institutions helpful in honing its understanding of the attackers and their attacks, helping it to avoid greater harm.

FINANCIAL SECTOR

1. Web Shell attack

Not all information sharing takes place through formal organizations dedicated solely to that purpose. For example, one financial institution first learned about attempts by a specific threat actor to inject a particular web shell multiple times, with the intent to gain control of their system and run further commands, when they were told about it directly by a government “partner.” The threat actor was unsuccessful, but the information that was shared with the financial institution was important and alerted the institution that a particular threat actor was attempting malicious activity. This is among the more direct and narrow versions of information sharing — single entity to single entity — but a success nonetheless.

2. Denial of Service Attacks on U.S. Banks in 2012-2013

Threat actors associated with Iran launched a series of potent distributed denial-of-service attacks on major U.S. banks, mainly in 2012 and 2013. These attacks frequently imposed tremendous costs on the banks that were attacked, as well as others that prepared to defend against such attacks.6

Attackers initially targeted individual banks, and evolved to target multiple banks at a time. Sometimes, in the minutes before an attack, government or private sector entities were able to see the attackers loading scripts containing information identifying which banks were targeted next in an attack. When available, this information was shared with banks in order to alert them of a potential imminent attack. Some who received the information were able to use those minutes to prepare well enough that, as a result, on some occasions the attackers just moved on to other targets because the banks had hardened their infrastructure or otherwise mitigated the attacks. The targeted banks who were involved in information sharing were often able to avoid substantial harm.

More generally, when these attacks began, and over the extended period they took place, as well as in the aftermath, information sharing between the banks and others, through FS-ISAC and with the government, expanded dramatically in important ways from what it had been before these attacks. The number of members and other participants sharing information in the financial sector expanded greatly, and the Department of Treasury worked closely with the sector. That increased collaboration and sharing benefited participants, and the expansion of information it spurred still benefits that sector today. Based on this experience, many in the sector also are preparing for and sharing information about possible attacks that could follow from the recent rise in tensions with Iran.

HEALTH SECTOR

1. Major Health Insurer

In 2014, a user within a major health insurer’s organization opened an email that contained malicious content. This phishing email allowed the attackers entry into the health insurer’s systems giving them access to information and opportunity to make changes.

The attack was discovered on a Tuesday, and by that Thursday, there was a flow of information being shared within a prominent ISAO. That ISAO moved quickly to alert members about the attack and the organization. It did not spread as it might have otherwise. The ability to alert community members about this potential threat within 48 hours — a threat responsible for one of the highest profile breaches in the sector — shows the speed at which information sharing can mitigate threats across a sector.

6 https://www.justice.gov/opa/file/834996/download
2. Ransomware

A particular strain of ransomware emerged that denied the availability of critical systems and information to many businesses, particularly in the health care sector. The damage it inflicted was particularly severe in the United Kingdom, where the national health care system utilized many out-of-date computer systems, and was behind in patching. One of several reasons (including discovery of a “kill switch”) that the impact of this ransomware attack was less severe in the healthcare sector in the United States, was that an information sharing organization serving the health sector received notification almost immediately from a member when the ransomware first appeared. That organization, with input from its members, began tracking, analyzing and putting alerts out to its members very quickly after it appeared, several days before the ransomware inflicted harm in the United Kingdom and attracted wide attention in the United States. Through information sharing, members knew very quickly about the threat, that it was spreading, and actions they could take to minimize the likelihood of serious harm, and had a better opportunity to address vulnerabilities and otherwise prepare.

TRANSPORTATION INDUSTRY:
AVIATION AND AUTOMOBILES

1. Aviation DDoS Attack

An aviation company experienced a DDoS attack. It shared information about it through the Aviation ISAC. A week later, another aviation company noticed signs of a potential DDoS attack and notified the Aviation-ISAC, who communicated with, among other members, the first victim. As a result, to help apply the lessons learned from the earlier DDoS attack, a cyber expert from the first victimized company who had been through the attack got on a plane and actually flew (international flight) to the location of the second aviation firm in order to help them work through the attack. That rapid response, which helped to solve the underlying problem, would not have been available or successful without information sharing. This episode also shows how information sharing relationships can build trust and potentially enable valuable knowledge and experience that can be leveraged for related kinds of cybersecurity collaboration, in this case for actual incident response. What is most noteworthy is that these two companies are competitors. The credo in aviation, given the interdependence of the global air transportation system from many perspectives, was “we will not compete on security” but rather build a safe and resilient global air transportation system.

2. A defense contractor

Information sharing between two defense contractors enabled a potentially serious threat to be mitigated. The second contractor discovered the intrusion, and established that the method of compromise appeared to be a key logger. The perpetrator was able to get into the network, unnoticed. Once inside, the adversary could access information such as passwords, contacts, and sensitive intellectual property. Depending on its objective, the perpetrator could potentially have caused other problems through its presence as well, such as releasing malware into the system.

The defense contractor immediately notified and shared information with others. Following up on that information, at least one other defense contractor discovered similar activity, and they were able to contain the perpetrator within the system. Both firms were able to address the situation quickly, and mitigate the threats. The second defense contractor was only able to conclude this diagnosis and mitigation as quickly, because a competitor shared this information with it.

3. Car Resale Security

This is an example where sector level information sharing has enabled the vehicle sector to protect the data of their customers. Car remarketers move and resell large numbers of vehicles. Those cars have increasingly offered entertainment and communications systems to owners, which can connect with their mobile devices. It is common now for car owners, by way of this mobile connection, to upload personal information and contacts into their cars. The reason an owner or regular passenger would do this is obvious — they want to call their friends and family, play their music, and otherwise customize their vehicle experience. For safety and other reasons, they would like to do as much as possible without the distraction of handling a phone and dialing. The industry has learned that this information is frequently still accessible in the car’s informatics systems after the owner has sold it, and it is in the possession of resellers. Historically, there has not been as easy a way for individuals to delete this information prior to resale, as there has been to upload it. This same problem can also occur in rental cars, where users also sometimes con-
to their mobile devices. Sector level information sharing has been used to spread awareness of this issue to auto companies, resellers, rental car companies, and increasingly even to consumers. Industry has urged customers to delete personal information before the resale of the car, but increasingly resellers and rental car companies are aware of the possibility that they are taking possession of personal data, if only accidentally.

**IT SECTOR**

1. **Heartbleed Vulnerability - March 2018**

A large technology provider that is a member of the IT (Information Technology)-ISAC sent IT-ISAC a request for information about a suspicious IP address geolocated in a foreign non-friendly country that it found on its network. IT-ISAC engaged with its partners at the NCCIC, which was able to confirm they also had seen instances of this or similar IP addresses trying to communicate in a similar way with other networks. Further research was able to link the IP addresses to a report entitled "OpenSSL TLS Malformed Heartbeat Request Found-Heartbleed."

A similar listing was also indicated in another government’s security operations center around December of 2017. A quote from the report stated “Mask and Crouching Yeti APT may have possibly been linked to Heartbleed activity.” The IPs have been known to exploit stolen keys over a period of up to 7 years. The report noted that until keys and certificates are replaced, the entity’s network, intellectual property, and customer data is still vulnerable. Furthermore, failing to remediate Heartbleed undermines other security controls, e.g., strong authentication and privileged access to behavioral analysis and network access, because attackers have the trusted status of valid keys and certificates to authenticate and cloak their malicious activities.

By sharing through IT-ISAC, the original target and other partners of IT-ISAC were able to confirm that the IP was malicious and associated with exploiting the Heartbleed vulnerability. Individual companies, especially the one that identified the IP on its network, benefited from information sharing with IT-ISAC and the U.S. government, and were able to quickly associate the IP with an ongoing threat.

2. **Golden Niagara/Gold Lowell-February 2018**

A member company asked the IT-ISAC what it knew about a threat named “Golden Niagara.” The IT-ISAC sent a request for information to members. An IT-ISAC member with a threat intelligence business was able to determine that "Golden Niagara" was a different name for the actor group known as “Gold Lowell.” Gold Lowell is the group that unleashed the SamSam Ransomware that impacted the City of Atlanta, the State of Colorado, and numerous other victims. The IT-ISAC was able to collect several reports from threat intelligence providers that had details about the threat actors and indicators associated with the SamSam campaign. These reports were also shared on the IT-ISAC’s threat intelligence platform so that all members could have access to the indicators.

The sharing member assessed that the sharing was very valuable and ultimately prevented harm. They — and other IT-ISAC members — received an updated consolidated set of indicators associated with an active, ongoing attack that was affecting other organizations. By collaborating with the IT-ISAC, they were able to confirm the actors involved, and obtain updated indicators associated with the active campaign to members, in order to improve their collective defenses.

**RETAIL SECTOR**

1. **Credit Card Points of Sale**

This involved sharing in both the finance and retail sectors. Bad actors were stealing sensitive information from point-of-sale systems. Certain fraudulent emails that linked from merchant systems to banks, and followed other patterns were detected, along with other tactics, techniques and procedures (TTPs) used by the perpetrators as part of their campaign. Information was shared among banks and, in both directions, with the Secret Service. The information shared about the TTPs of the attackers, and the collection of best practices to avoid harm from these attacks, was shared and incorporated into a paper made available by one of the ISACs. This helped retailers that transacted business with the public through point-of-sale credit card systems to protect those systems and consumers better, and more successfully face and avoid some of these threats.
2. Cobalt Gang/Cobalt Group

This involved a large retail company that engaged in information sharing with R-CISC (formerly Retail Cyber Intelligence Sharing Center, now RH-ISAC, Retail and Hospitality Information Sharing and Analysis Sharing Center), FS-ISAC, and other information sharing organizations. In the middle of November, several years ago, the retailer detected command-and-control call-outs from their networks. The November season is a high stakes period for retailers, in the run up to the holiday season in the United States. The rules the retailer’s intrusion detection systems were using generated significant numbers of false positives, so they initially did not panic. The attack seemed to involve a brand new Java Script RAT (Remote Access Tool). As part of its analysis, the retailer also looked back, and learned that one week earlier it also seemed to have been phished by the same attacker. The retailer then realized that it had been targeted twice, one week then the next. The retailer shared in detail with the R-CISC, and with some of its other ISACs about the later attempt.

With the help of information that had been shared, the malware was spotted. The particular malware was attempting to bypass application whitelisting. The perpetrator was known as a criminal group sometimes called the Cobalt Gang. The retailer was able to track it to a resume that had been submitted online, as part of a job application through an online employment job board. Research through the information sharing organization showed that as many as 30 retailers were targeted. Research by R-CISC and FS-ISAC with their members on these incidents was also able to identify some malware.

The large retailer that initiated this sharing also had a relationship of trust with and engaged in some sharing directly with some other major retailers, outside of the ISAC framework. The major retailer had a direct dialogue with at least three other retailers about this particular threat that it was the first to share — those major retailers told it that they were able to avoid harm because of the quality, reliability and nature of the information that had been shared.
Sources


* All quotes in this section are from the following source: MS-ISAC Representative (2018). Success Stories in Cybersecurity Information Sharing (SSCIS) conference. October 23. Albany, NY.