IBM Security

Cybersecurity for state and local governments: Protecting public infrastructure

IBM® X-Force® Incident Response and Intelligent Services (IRIS)

Special Intelligence Report Q4 2019

IBM

Threat perspective: Cyber resilience in local government

Special Intelligence Report Q4 2019

Threat perspective: Cyber resilience in local government

Introduction

US citizens rely on state governments and local municipalities to provide a host of services—everything from access to public records, police protection, and education and welfare, to voting and election services, which allow citizens to participate in their democracy. As technology advances, so does the citizen-consumer's demand for an increasing number of these services to be provided digitally. State and local governments have responded to the demands by increasingly modernizing digital access to the services they provide. While this digital transformation grants ease of access to citizens looking to engage state-funded online programs and services, it potentially increases vulnerabilities inherent to public-facing systems.

While many state and local C-suite-level officials have incorporated information security and data protection measures into their infrastructure, the data collected by the state and the types of services it offers citizens represent a unique attraction for cyber criminals. Thus, it requires an equally unique approach to ensure the protection of critical state and municipal digital systems, which necessitates funding and supportive policies.

According to a survey conducted by the International City/County Management Association, 44 percent of municipality and county respondents felt greater funding for cybersecurity was needed to ensure the highest levels of cybersecurity, 38 percent cited the need for better cybersecurity policies and a further 38 percent called for greater cybersecurity awareness among local government employees.[1]

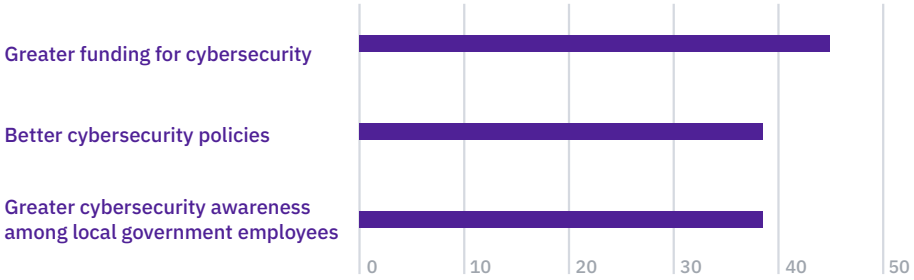

Figure 1: Top three things local governments need most to ensure the highest level of cybersecurity[2]

Although the appropriation and approval processes are often prolonged, time is of the essence for state and local governments facing advanced cyber threats. Data beaches that affect the public sector have been reportedly carried out by adversaries ranging from cybercriminal groups to state-sponsored threats.[3] These breaches have also been taxing the economy with losses measured in billions of dollars every year.

Breaches potentially cost the public sector $1.35 billion in 2018[i 4,5]

[i] According to the Identity Theft Resource Center's (ITRC) 2018 Annual Report, data breaches in the government sector (99) resulted in the exposure of about 18 million records. The IBM-sponsored Ponemon Institute 2019 Cost of a Data Breach report discovered the average cost of a lost record within the public sector was $75, based on breach events occurring between July 2018 and April 2019. If the industry applies the average cost based on Ponemon's research to the number of records lost, the total loss, based on cost per record, could have potentially reached $1.35 billion.

Please note: Estimates generated by X-Force IRIS are derived by multiplying the average cost per record lost by industry as prescribed by annual Cost of a Data Breach reports issued by the Ponemon Institute, and don't reflect the exact methodology developed by the Ponemon Institute. Exact figures may be lower for some breaches, which may have occurred prior to the publication of Ponemon's findings. Also, Ponemon's estimates don't include breaches in which more than 100 thousand records were compromised, which may result in lower, actual costs per record. For further details on Ponemon's costing methodology, known as activity-based costing (ABC), please visit https://databreachcalculator.mybluemix.net/how-we-calculate-the-cost.

The response from government agencies regarding cyber-related events hasn't always been adequate; the US Senate documented frequent failures in federal cybersecurity to apply even basic policies and controls that would otherwise help mitigate looming risk.[6] To address the challenges endemic to local government information systems and reduce the level of vulnerabilities, a full spectrum cyber resilience plan must be integrated into every state and local government security strategy.

In this special report, IBM® X-Force® Incident Response and Intelligence Services (IRIS) explores the current operational environment of state and local government sectors, adversarial activity targeting those sectors, and the implications this evolving threat landscape has on cyber resilience at the state and local government level.

The big picture

According to a 2019 survey conducted by the National Association of State Chief Information Officers (NASCIO), security and risk management sit firmly at the top of state chief information officer (CIO) priorities.[7] And rightfully so, as the average cost of a data breach in the United States has risen from $3.54 million in 2006 to $8.19 million based on the 2019 IBM-sponsored Ponemon Institute *Cost of a Data Breach Report.*[8] Moreover, the accelerated number of ransomware attacks against state infrastructure in the last calendar year alone will almost certainly increase this average.[9] In May 2019, a single ransomware attack that struck Baltimore, Maryland, ended up costing the city $10 million in technological upgrades, and $8.2 million in lost revenue.[10]

Digital transformation in the sector

Information technology has become a primary medium for citizens to interact and engage with their state and local governments.[11] As these agencies move towards implementing paperless environments and furnish their members, staff and constituency with consumer-grade online experiences—not to mention keep eager students apprised of school closings at the first signs of snowfall—the availability of their services, the integrity of the information, and the confidentiality of citizens' personal data will only become more critical over time. This transformative change, pushed along by constant advances in technology, has driven local governments to continually create and adopt public-facing applications that collect, use, store, and transmit data.[12] These changes mean that, aside from relying on information systems to ensure the lights stay on and the water is safe to drink, local governments host and transfer vast amounts of personally identifiable information (PII), from birth certificates to criminal records, financial data from tax and insurance information to those paid parking tickets, and even sensitive electoral data.

Threats from criminals and nation-states abound

For cybercriminals looking to turn a profit, the data troves that government agencies store on local residents holds the promise of PII-rich records that can be used in identity theft and numerous fraud scenarios. For state-sponsored threat actors looking to collect confidential information, or even to disrupt and potentially destroy critical infrastructure, state and local government networks represent high-value targets that may satisfy multiple objectives.

Today, the targeting and frequency of assaults on local government networks occur at a staggering rate. As of April 2018, the digital infrastructure of the state of Minnesota is probed about three million times per day, according to government IT officials.[13] In the same year, results from a survey conducted by the International City/County Management Association, revealed that 60 percent of local governments that are aware of the frequency of attacks, incidents or breaches on their IT systems reported their networks are subject to daily, almost hourly assaults.[14]

Challenging circumstances

While digitization projects advance across the sector and threats continue to escalate, almost every state and township faces the challenges of garnering the appropriate funds to modernize outdated systems and compete with the private sector for a limited pool of skilled information security workforces. Meanwhile, the limited number of network defenders currently at the local government level must work feverishly to patch networks, educate their heavily targeted users against clever—and even not so clever—phishing campaigns, field new digital applications, manage data privacy, and keep online services running—all while updating the town's local event page, and preventing website defacement and digital vandalism.

Unfilled cybersecurity jobs are expected to reach 1.8 million by 2022, up 20 percent from 1.5 million in 2015, according to the Center for Cyber Safety and Education.[15] The dearth in skilled security professionals increases the demand and compensation for experienced workers, making it challenging for government agencies to hire and retain top talent. In addition, the heavy cost of modernizing infrastructure with the analytic tools and security controls necessary to mitigate today's sophisticated threats is another significant drain on the government purse.

Sharpening the focus on readiness and resilience

Malicious cyber activity against critical infrastructure can move far beyond the discomfort of delayed online updates to current legislation, or a brief return to the handwritten check, while online portals become functional again. Should a local government become the victim of a cyberattack or breach, citizens could face consequences that are far more dire than a simple inconvenience, such as:

— Hospital operating rooms could potentially face blackouts during critical patient procedures.[16]

— Police and other first responders could be unreachable and unable to respond to crises.

— Local universities could lose decades of intellectual property and research.

— District attorney offices and police departments could lose critical operational data.[17]

— Citizens' personal information, including biometric data like fingerprints, could fall into the hands of malicious actors, potentially resulting in a lifetime of fraudulent identity challenges.

Breaking down this complicated and complex attack surface, this report identifies some of the key cyber-enabled industries unique to state and local governments. Each section provides a general overview of activity, key exemplars of breach events, and the current outlook and over-the-horizon threats from the X-Force IRIS perspective. To gain insight into the general cost of malicious cyber events per local government segment, X-Force IRIS applies the average cost per a compromised record by industry as prescribed by the 2019 Ponemon Institute report to generate the potential cost of an event to state and local government.[ii] The five segments include:

— Local government

— Emergency services

— Healthcare

— Education

— Election security

To learn more about the IBM Security Command Center, please visit:
ibm.com/security/services/managed-security-services/security-operations-centers

[ii] Please note: Estimates generated by X-Force IRIS were calculated by multiplying the average cost per record lost by industry as prescribed by annual Cost of a Data Breach reports issued by the Ponemon Institute. For further details on Ponemon's costing methodology, known as activity-based costing (ABC), please visit https://databreachcalculator.mybluemix.net/how-we-calculate-the-cost.

Top targets in the government sector

Top targets in the government sector

Local government agencies

City, state and local governments have a vast amount of responsibilities when it comes to providing services to citizens. While state legislatures and town councils introduce laws and legal code to foster a secure and thriving economy, state and local governments also guarantee that citizens and businesses have access to fundamental utilities, such as water, gas and electricity; safe repositories for public records, such as leases, licenses and property; and reliable public transit to name a few.[18]

Targeting payroll and human resources

At the state and local level, criminal actors test the locks on potentially profitable government targets, like those in payroll and human resources (HR). One reason these systems are lucrative is that they often contain not only payroll, but also HR and benefit information for every government employee. That information may include PII, such as names, addresses, social security numbers, and bank account information.

Potential cost of an HR-related breach associated with the Minnesota SEMA4 System: $2.7 million (2017)[iii 19]

Breaches of third-party payroll and HR providers through phishing attacks have led to the compromise of sensitive data and the direct theft of money.

The ongoing use of legacy systems and outdated software can increase the vulnerability and exposure of this PII to potential attacks. In 2018, the Minnesota CIO acknowledged that one of the state's payroll systems containing PII, such as 38,000 state employee social security numbers, is running on 15-year-old software.[20]

[iii] In an infographic released by the state of Minnesota employees' payroll office, the information of about 38,000 employees was housed in the Statewide Employee Management (SEMA4) system in 2017. Applying cost per record from the Ponemon Institute 2017 Cost of a Data Breach report, which rates the average cost per record lost in the public sector at $71, the state of Minnesota estimates that a compromise of SEMA4 could have resulted in a potential cost of $2.7 million.

Agency	System name	Age of system (years)	Age of oldest hardware (years)	System criticality (according to agency)	Security risk (according to agency)
Defense	System 1	14	3	Moderately high	Moderate
Education	System 2	46	3	High	High
Health and Human Services	System 3	50	Unknown	High	High
Homeland Security	System 4	8 – 11	11	High	High
Interior	System 5	18	18	High	Moderately high
Treasury	System 6	51	4	High	Moderately low
Transportation	System 7	35	7	High	Moderately high
Office of Personnel Managment	System 8	34	14	High	Moderately low
Small Business Administration	System 9	17	10	High	Moderately high
Social Security Administration	System 10	45	5	High	Moderate

Figure 2: The 10 most critical federal legacy systems in need of modernization[21]

Given that state and local governments must continue to host and transmit high-value data pertaining to payroll and HR, those associated networks will continue to be a target to cyber threats. The modernization of legacy systems, adequate role-based training for employees, and the proliferation of up-to-date standards for the use and storage of sensitive data can help harden government systems and reduce the overall attack surface.

An example of that sort of progress comes from the state of Hawaii. After 50 years of manual processing and using legacy machines, the state has completely modernized its payroll system.

Hawaii's state offices not only benefit from reduced long-term costs and an improved user experience, but also avoid the risks inherent to legacy systems that often remain unpatched and are increasingly vulnerable to attack.[22]

June 2018:

The third-party HR service BenefitMall, also known as Centerstone Insurance and Financial Services, supporting the Delaware Department of Insurance, experienced a five-month-long data breach, impacting at least five companies and the personal data of about 650 Delaware residents.[23] In January 2019, BenefitMall notified a further 111,589 consumers who were potentially impacted.[24]

March 2019:

An email appearing to originate from a Tallahassee, Florida city manager, was sent to an undisclosed recipient. The email, which was crafted with a Dropbox link containing malware, was opened by the recipient and ultimately allowed attackers to compromise the city's payroll network.[25]

April 2019:

In a separate incident, Tallahassee fell victim to a cyber theft of $498,000. The attacker was able to breach the city's third-party payroll service provider and reroute the direct deposit paychecks of about 200 employees to an actor-owned account.[26]

Targeting the transportation sector

Transportation is a vital component of economic and national security, global trade, and passenger travel, representing a high-value target for cybercriminals and state-sponsored threats. Depending on the sophistication, scale and frequency of attacks, cyber incidents in this space have the potential to put human lives at risk. They can also disrupt critical services, damage or destroy highly specialized equipment, and ultimately inflict detrimental cascading effects upon multiple downstream industries.[27, 28]

When it comes to the resilience of the transportation infrastructure in the US, Americans may have a genuine cause for concern. Quoting the results of a survey conducted by Pew Research in 2019, 83 percent of Americans think it somewhat to very likely that a malicious cyberattack would result in damage to public infrastructure.[29]

While information held by transportation systems presents an attractive target for cybercriminals, arguably the most critical asset at risk is the functioning of the transportation infrastructure itself. Disrupting the operations of the transport system can take many forms, but the most common thus far has been ransomware attacks.[30]

The first instance of ransomware emerged over 20 years ago and the first ransomware attack on a local government can be traced all the way back to 2013. The accelerated number of attacks in the last 24 months in this sector potentially points to a new evolution in the cyber threat landscape, to include the targeting of local public transportation.[31, 32]

In the United States, the transportation sector supports nearly 10 percent of American gross domestic product (GDP).[33] To reduce costs and optimize processes, a growing number of critical systems surrounding the transportation sector have gone "online" through digitization and automation to support operations and customers.

With eyes on the horizon, as municipalities work to become smart cities—in which most infrastructure is connected to the internet, including traffic lights, water systems and vehicles[34] — the transportation sector must re-evaluate its threat landscape and risk profile, and rethink resilience plans from the ground up.

November 2016:

On Thanksgiving and Black Friday, ransomware struck thousands of Windows systems used by the San Francisco Municipal Transportation Agency (SFMTA). While the attack compromised over 2,000 payment and scheduling systems, officials had to order all Muni gates be left open until IT personnel could clear the infected systems. Thank you, Muni, for the free fares and limited impact to commuters, although the government incurred about $559,000 per day in losses for uncollected fares.[35]

November 2017:

The Sacramento Regional Transit (SacRT) transportation agency experienced a breach in which a malicious hacker defaced the agency's online portal. SacRT was forced to shut down the site that accepts credit card payments and assigns buses and trains to routes.[36]

March 2018:

The city of Atlanta, Georgia was crippled due to a ransomware attack. For at least five days, critical functions were halted. City employees were unable to access the internet or email, residents were unable to pay bills online, and wifi access at the Atlanta Airport and city jail was shut down.[37]

September 2018:

On September 26, 2018, the Port of San Diego issued a statement that it had experienced a cybersecurity incident disruptive in nature. Although the port continued operating, port workers had limited access to administrative IT functions, causing temporary impact to public services, specifically parking permits, public record requests and business services.[38]

The Port of San Diego is considered a critical part of the US transportation infrastructure and network of maritime ports, being a commercial port, as well as a designated strategic port for the US Department of Defense (DoD). In late 2018, a federal grand jury in New Jersey indicted two Iranian hackers implicated in that attack and in similar extortion attacks on American organizations.[40] In 2019, it was revealed that the disruptive attack that affected the port was caused by SamSam ransomware, followed by a demand for payment in Bitcoin.[39]

Targeting utilities

In 2015, the University of Cambridge and Lloyd's of London published a report in which they found that a cyberattack on the United States' electric grid could leave 15 states and 93 million people between New York City and Washington, DC without power. The total impact to the US economy was estimated between $243 billion and $1 trillion, potentially leading to direct damage to assets and infrastructure, loss in sales revenue to electricity supply companies, and disruption to the overall supply chain.[41]

In 2016, a Manhattan US attorney announced charges against seven Iranian nationals who hacked the systems of utility companies in the US, including the Bowman Avenue Dam in Rye, New York.[42] Utility networks have also been subject to adjacent attacks impacting the local government's ability to accept payments for permits, licenses, fines, and utility use.

The growing demand and rapid adoption of smart technology into existing municipal infrastructure enables resident services, tourism, and economic expansion.[43] According to a study conducted by Grand View Research, Inc., the global smart cities market may reach $237.6 billion by the year 2025. On the other hand, the collection and transmission of vast amounts of data through connected systems creates a highly profitable target for criminal actors seeking illicit gain, and for state-sponsored actors who may be after monitoring capabilities.

As cities look to implement the most advanced technologies to update operations and service delivery, cybersecurity must be an integral part of the plan. To stay ahead of threats, some states like Connecticut have wisely invested in annual employee training and preparedness assessments.[44] Fostering a culture of cyber awareness can help enable key stakeholders to appropriately recognize, respond and mitigate the effects of a cyber emergency.[45]

January 2017 - August 2019:

A malicious actor compromised the Click2Gov payment portal for permits, licenses, fines, and utility use for Hanover County, Virginia residents, obtaining credit card information.[47] Two separate incidents in 2017 and 2018, resulted in the compromise of the portal, impacting multiple cities across the US, and seeing the loss of 300,000 payment card details. In August 2019, the portal was breached yet again, affecting two additional cities and resulted in the leakage of tens of thousands of records to the dark web for illegal sale.[48]

October - December 2018:

Topeka, Kansas experienced a cyberattack on the city's "pay online" site for water bills and other utilities. The compromise exposed the information of as many as 10,000 residents, all of whom received notifications, although forensic investigators haven't confirmed data misuse.[46]

August 2019:

The bill-pay website of the Murfreesboro, Tennessee water department experienced a cyberattack. The portal was defaced with an image of the Iranian flag and a Guy Fawkes mask, captioned with the phrase "Hacked by Iranian Hackers," among other messages. The incident appeared to be exclusive to the city's water department bill pay.[49]

Targeting the Department of Motor Vehicles (DMV)

According to the Identity Theft Resource Center's annual report, DMV data was exposed in a total of 175 breach events spanning across five industries in 2018 alone.[50] The DMV is an especially lucrative target for attackers as a vast amount of DMV data is stored and shared between multiple state agencies and third-parties, potentially providing malicious cyber actors an extended attack surface. PII-rich records are in high demand as they can allow criminals to carry out fraudulent activity, such as the collection and sale of PII on illegal underground forums like the dark web and using it in a plethora of identity theft and fraud scenarios.

To gather their own caches of DMV-like data, malicious cyber actors also develop legitimate-looking web pages purporting to provide DMV services, such as driver's license applications and vehicle registrations. These fake phishing sites are developed to obtain PII and customer credit card numbers and may be easier to mount than a direct attack on the DMV.

Having the strategic conversation on prominent threats and vulnerabilities associated with DMV data with key state-level stakeholders, congressional delegates, cybersecurity experts and vendors providing critical software and hardware is necessary to establish systemic network security. To address the level of security surrounding the data collected and maintained by the DMV, several states have begun stand-up councils and workings groups.[51] This approach is a wise strategy on the part of the states given that cybercriminals have proven able to target DMVs, their third-party service providers, and the DMVs' sister agencies to breach and exfiltrate data.

June 2018:

The third-party vendor of the Department of Highway Safety and Motor Vehicles (DHSMV), Unisoft Communications of Miami, was under investigation regarding the improper use of PII associated with Florida's licensed drivers, which encompassed roughly 17 million drivers. In 2016, Unisoft was flagged for posting easily accessible PII protected by the Federal Driver Privacy Protection Act (DPPA) to its public-facing website, mydrivingreport.com.[52]

October 2018:

The California DMV sent out a warning regarding fraudulent websites impersonating the DMV that were attempting to charge customers for completing electronic driver license and ID card applications, making DMV appointments, and other online transactions. In some instances, the fake websites contained user agreements in which consumers provided the attackers with permission to access and use their personal information, including the sale of personal details for profit.[53]

December 2018:

The Pennsylvania Department of Transportation (PennDOT) also issued official warnings to customers planning to renew their driver's licenses or vehicle registrations on the PennDOT website. The warning informed users of fake DMV sites or websites that look official and charge people for services that PennDOT offers for free.[54]

January 2019:

The Minnesota License and Registration System (MNLARS) accidentally shared the private information of 1,500 residents with three firms authorized to buy vehicle data.[55]

March 2019:

The El Paso County Office of the Clerk and Recorder in Colorado Springs issued warnings to citizens about fake websites involving online vehicle renewals. The sites were being used to steal personal information and credit card data, as well as charge customers for fraudulent services.[56]

May 2019:

Illinois Secretary of State's office and the City Clerk of Chicago's third-party vendor Electronic License Service LLC (ELS), authorized to sell vehicle stickers at currency exchanges, was compromised and exposed information hosted on a development server to the internet.[57] Information on the server included resident data and a .git file potentially hosting database access credentials. ELS has access to government systems and the personal information of hundreds of thousands of customers.

Targeting biometrics and REAL ID

The biological and physiological traits of individuals can be used to create a unique biological signature, which can be captured in biometric data.[58] At the state and local level, biometric data is being baked into the issuance of driver's licenses, specifically in the new REAL ID project, requiring the inclusion of photographs that keep to a biometric standard, allowing for facial recognition and authentication.[59] The inclusion of this new data set, combined with existing PII already collected for the issuance of driver's licenses, presents an attractive target for cybercriminals. Access to this rich data set can provide multiple ways for criminal actors to impersonate individuals.

Since 1924, US federal law enforcement has collected and managed a nationwide fingerprint collection used to uniquely identify individuals and attribute criminal events. Today, federal organizations have access to vast amounts of biometric and biographical data, including fingerprint data, face and vocal recognition data, and DNA. Depending on authorization and need, these repositories are shared with domestic and international law enforcement partners through various platforms.[60]

While biometric data can be an excellent source for secure authentication, the loss or compromise of these details represent a significant, continuous identity threat. Unlike passwords or even social security numbers, biometric data can't be changed once it's exposed or stolen.

March 2014:

In a major data breach, the United States Office of Personnel Management was compromised, exposing the personal data of 21.5 million government employees and applicants, as well as the data of their spouses and close relatives. Personnel data collected over the course of 30 years was compromised, including biometric data.[61]

August 2019:

Six states reported that the fielding of the REAL ID program has been accompanied by technical glitches, delays hindering a smooth project rollout, and miscommunication between state motor vehicle departments and the Federal Department of Homeland Security (DHS) regarding needed documentation. Other states have yet to comply due to growing privacy concerns.[62]

August 2019

Security researchers discovered an unencrypted database related to the platform Biostar 2, used by thousands of organizations to control visitor management systems and secure access. The breach exposed over 27.8 million records and a total of 23 gigabytes of data, including fingerprint data and facial recognition information.[63]

Emergency services

Targeting law enforcement

The proliferation of digital technology brought with it a new medium for conducting criminal activity and new challenges for local law enforcement.[64]

While continuing to carry out traditional duties in the kinetic environment and adjusting methods to investigate and uphold justice in a cyber environment, police officers face the additional responsibility of defending sensitive networks housing critical PII, evidence and case-related data, and biometric information. These new duties are no less important than protecting themselves, their families, their stations and the districts they're assigned to.

Strategically, uniformed officers use a variety of technologies to detect the tools used by criminals to conduct or facilitate illicit activity. In 2016 alone, cybercrime cost the American economy as much as $109 billion.[65] According to the Federal Bureau of Investigation (FBI) 2018 Internet Crime Report, victim losses from reported cases totaled $2.71 billion.[66]

To investigate cyber threats and track down criminal actors, law enforcement requires access to sensitive information hosted on police networks.[67] The use of shared digital infrastructure to communicate, collect, store, and access critical data remotely, can greatly facilitate strategic communication for law enforcement and emergency services.[68, 69] However, the potential disparity in implementation and security controls, which may vary by state and local jurisdiction, present threat actors with multiple vectors for gaining illegal access into highly sensitive, police-specific systems designed to help uphold public safety.[70]

December 2018:

The police department of the Township of Maplewood, NJ, detected suspicious network activity and hired a third-party forensic team to investigate, uncovering malware on the network. Although it was inconclusive whether any information was accessed, the department's network houses PII that includes local residents' social security numbers, driver's license numbers, financial data on payment cards and bank accounts, along with access codes and passwords to these accounts.[71]

April 2019:

The FBI National Academy Associates, Inc. (FBINAA) publicly announced that three associated websites, a coalition of different chapters across the US, had been compromised, resulting in the exfiltration of approximately 4,000 personal information records, which the hackers subsequently offered for download on their own website. To show additional compromise, the hackers sent the link of another chapter's website, defaced with a screenshot of an encrypted chat they had moments earlier. They claimed to have used public exploits to indicate which websites had outdated plug-ins. The attackers' self-proclaimed motivation was "experience and money."[72]

May 2019:

A Riviera Beach Police Department employee opened a malicious email introducing a virus into the city's computer network. The city's system-wide email and direct deposit services were shut down, forcing paychecks to be hand-printed. To regain a foothold, the council authorized the purchase of 310 new desktops, 90 laptops, and additional hardware, collectively costing $941,000 with a $341,000 bill rolled over to the taxpayer.[73]

July 2019:

The IT agency supporting the Los Angeles Police Department (LAPD) reported that it had been contacted by a malicious actor who had gained unauthorized access to and downloaded the personal information of about 2,500 LAPD officers, trainees, recruits, and 17,500 police job applicants. The malicious actor provided the IT agency with examples of data as evidence of the compromise, including personal and financial information.[74]

August 2019:

The FBI announced the ongoing investigation into the compromise of the Oklahoma Law Enforcement Retirement System (OLERS). The $1 billion pension fund provides support to about 1,500 beneficiaries, all retired Oklahoma state government state troopers, public campus police, and park rangers.[75] The breach occurred in late August 2019, when a malicious actor broke into a single email account and stole roughly $4.2 million from the pension fund.[76, 77] Two years earlier in 2017, a similar fate befell the Iowa Public Employees' Retirement System (IPERS). Online criminals obtained stolen social security numbers and birth dates to register for IPERS accounts and altered the direct deposit information of 103 beneficiaries to collect payments.[78]

Targeting first responders

When discussing the topic of cyber vulnerabilities of police departments, informed conversations must consider services beyond officers of the law to include public safety as a whole, including paramedics, disaster response teams, and firefighters, to name a few.

According to a March 2019 report by the National Fire Protection Association, in 2017 an approximate 1,056,200 firefighters in the United States supported an estimated 29,819 fire departments nationwide.[79] To reach any firehouse or local police department, anyone in America can dial the number 911—unless the dispatch system is down. The network breach of emergency services can result in the downing of dispatch and strategic communication systems, and the exposure of the personal data of patients or residents.

According to the National Conference of State Legislatures, approximately 240 million emergency calls are made per day in the United States, distributed to 100,000 emergency dispatchers in nearly 6,000 public safety answering points (PSAPs). The 911 emergency system has been the primary emergency contact for the American public for over 50 years now, with 80 percent of calls originating from wireless devices.[80] This critical system has been reliable, but it's becoming more outdated and vulnerable over time. With this widespread evolution of technology, state and local governments acknowledge the need to replace the legacy system, which is an understanding that has resulted in more than $109 million in grants issued to 34 states, and two tribal nations to help modernize 911 call centers.[81]

The installation of new next-generation 911 (NG911) and FirstNet systems to transmit voice calls, photos, text, and video content, will occur at the individual state, regional, and local levels, and require an abundance of contractors to host and provide digital services.[82, 83] Traditional 911 services operate on internal networks with little to no connection to other digital platforms. However, NG911 interconnects multiple networks, which can also expand the attack surface for malicious actors who might plan to disrupt or disable PSAP operations.[84]

As evident by the digital compromise of industrial supply chains, the breach of any partner organization can potentially enable upstreaming attacks by cyber threat actors.[85] Thus, if a third-party providing digital services that support first responder applications experiences a breach, criminals may use that illegal access to gain entrance into numerous connected systems within the greater NextGen environment. With this kind of access, cybercriminals and nation-state adversaries could harvest vast amounts of actionable PII data, manipulate or influence evidence and investigations, and potentially disrupt critical infrastructure, disable access or destroy sensitive data.

March 2018:

Baltimore, MD suffered a breach impacting the city's computer-assisted dispatch (CAD) system, forcing dispatch workers to handle calls manually.[86] This incident is familiar to Henry County, Tennessee, as it faced a similar situation in June 2016, when it was hit with a ransomware attack on a 911 call center, disabling the center's dispatch system, and forcing employees to manually track emergency calls with only paper and pen.[87]

April 2018 - May 2018:

Ohio's Riverside Police Department (RPD) in April 2018, and in May 2018, the Riverside Fire Department (RFD), were struck with ransomware. In the April attack, unauthorized users compromised the network and encrypted data regarding ongoing investigations. In May, malicious users installed malware on the network, leading to another ransomware infection.[88]

August 2019:

The Fire Department of New York (FDNY) notified 10,253 patients, whom the FDNY Bureau of Emergency Medical Services (EMS) had previously treated, that their personal information may have been compromised due to the loss of an employee's personal external hard drive. The employee had authorized access to the information, but had, unfortunately, also uploaded it to their personal drive, which then went missing.[89]

Education

From pre-kindergarten to public universities, state and local governments fund, support, and facilitate the operation of public schools across the country,[90] which provides students with a safe place to learn, grow, and develop their interests and talent.

Throughout the public education sector, digital systems are being used to host sensitive student data, from enrollment to transcripts and financial information, along with large amounts of original research created in state universities. For online criminals, the PII data of students can be a source for creating fraudulent personas to conduct illegal activity.

For state-sponsored threat actors, the compromise of higher-education targets can furnish their own nation's domestic technology development,[91] as university networks can host sensitive medical and military research, commercial intellectual property, and be a medium for upstreaming into trusted partner environments.[92]

Breaches potentially cost the education sector about $200 million in 2018[iv 93, 94, 95]

From state-sponsored threat actors targeting cutting-edge research to criminal threats looking to harvest or expose sensitive PII data, educational institutions will continue to face a host of cyber threats.

In addition, the large number of government agencies, commercial organizations, third-party service providers, and student and faculty users with access to education systems provide threat actors with a multitude of vectors for conducting malicious activity. This issue can be especially problematic if the large and heterogeneous userbase in the education sector is harder to centralize with security governance. For instance, students may be accessing their accounts from compromised devices and they can easily, unknowingly open attachments carrying malware on internal networks when inside their institution's walls.

It will likely take the joint efforts of local government and academia to identify and address vulnerabilities in this sector and to continually fortify its sensitive networks.

Mitigation plans can be implemented at the university level. Augusta University provides a positive example for having implemented multifactor authentication, banning protected health data from emails and adopting email screening software to detect the presence of protected health and personal data.[96]

[IV] According to the Identity Theft Resource Center (ITRC) 2018 Annual Report, data breaches in the education sector (76) resulted in the exposure of about 1.4 million records. The IBM-sponsored Ponemon Institute 2019 Cost of a Data Breach report, discovered the average cost of a lost record within the education sector was $142, based on breach events occurring between July 2018 and April 2019. If the industry applies the average cost based on Ponemon's research to the number of records lost, the total loss, based on cost per record, could have potentially reached $200 million.

Please note: Estimates generated by X-Force IRIS are derived by multiplying the average cost per record lost by industry as prescribed by annual Cost of a Data Breach reports issued by the Ponemon Institute, and don't reflect the exact methodology developed by the Ponemon Institute. Exact figures may be lower for some breaches, which may have occurred prior to the publication of Ponemon's findings. Also, Ponemon's estimates don't include breaches in which more than 100,000 records were compromised, which may result in lower, actual costs per record. For further details on Ponemon's costing methodology, known as activity-based costing (ABC), please visit https://databreachcalculator.mybluemix.net/how-we-calculate-the-cost.

2013 - 2019:

Since at least 2013, Iranian state-sponsored threat actors associated with the Mabna Institute, tracked by X-Force as Hive0082, coordinated a cyber campaign compromising over 320 universities, of which 144 were US universities,[104] successfully exfiltrating over 30 TB of data.[105, 106] Between July and August 2019, the Mabna Institute targeted previously compromised education resources, sending library-themed phishing lures that pointed to spoofed login pages associated with the targeted institutions, aiming to compromise access credentials.[107]

November 2014 — September 2017:

Between 2014 and 2015, ITG09 advanced persistent threat (APT) group, which shares overlap with Leviathan, targeted US universities that provide naval-defense-related research to the US military.[97, 98] The operational timeline of these campaigns coincides with the drafting and release of the Made in China 2025 initiative, which names domestic high-tech shipbuilding as a manufacturing priority.[99]

In 2017, ITG09 targeted several US research and engineering institutions, and academic organizations associated with the maritime industry.[100, 101, 102] Phishing lures were sent to US defense contractors as part of that attack, specifically contractors at US university research centers with ties to the US military.

September 2017:

Augusta University Health employees responded to phishing emails soliciting login credentials. These unwitting actions resulted in granting attackers unauthorized access to 24 university administration and faculty staff member accounts. In July 2018, investigators determined that following this incident, malicious actors may have had access to the PII and protected health information (PHI) of about 417,000 people, including faculty, students, and patients throughout Georgia.[108]

November 2018:

An employee of the Chesapeake, Virginia school district opened a phishing email exposing the network to malware. Grassfield High School was highly impacted because its classes use technology more frequently, such as the economics class that is entirely comprised of computer-based learning.[109]

March 2019:

The breach of a Georgia Tech web application[110] was the second it suffered in less than a year. The breach exposed the PII of 1.3 million people, including current and former students, faculty, and staff members.[111]

April 2019:

The Mirrorthief Group, tracked by X-Force IRIS as Hive0084, injected a malicious skimming script into 176 US college and university merchandise online stores. The skimming script was injected into the shared JavaScript library on the e-commerce platform PrismWeb, which is used by the online stores. Mirrorthief potentially accessed payment card information to include names, card numbers, expiration dates, and card verification codes.[112]

May 2019:

New Jersey's Paterson Public Schools experienced a breach in which 23,103 account passwords and computer access tokens were obtained. This number includes credentials of all district employees.

At the time of reporting, it was unclear how the malicious user accessed the district's system. Three days after discovering the incident, the unauthorized user contacted the Paterson Times using a fake email address claiming the user had access to all system information, but the email was ignored. By the following Saturday, the actor provided evidentiary screenshots of two employee Outlook email inboxes, proving the actor was in possession of tens of thousands of district account credential sets, including those of former employees.[113]

July 2019:

Virginia's Shenandoah County Public Schools experienced a breach through a third-party software provider, AIMSweb 1.0. AIMSweb 1.0 is a platform used by students to take assessments, which teachers then use to determine the need for administrative services and planning. Student information exposed in the breach included names, some birth dates, and in some instances, email addresses. Administrative information compromised included names, job titles, work emails, and work addresses.[114]

August 2019:

Naperville, Illinois Indian Prairie School District 204 experienced a breach in which the personal information of 49,000 students and 2,300 teachers was exposed. The breach started at a third-party provider that handles the districts' K - 8 academic assessments. That vendor, Pearson Clinical Assessment, stated that the breach was limited to the first and last names of students, as well as birth dates in other cases. It also stated that no other identifying student information was accessed. For the 2,300 staff members, the data that was exposed included their first and last names, and school email addresses.[115] Several other schools were also among the 13,000 Pearson clients impacted by the incident.[116]

Healthcare

To facilitate nationwide programs like Medicaid and the Children's Health Insurance Program (CHIP), state and local governments must have access to varying levels of PII and PHI data.[117, 118] Electronic medical records (EMRs) and electronic health records (EHRs) can help give providers an accurate picture of an individual's health history and can be accessed in a variety of settings[119] through shared network infrastructures. These platforms house critical PII and PHI, detailing an individual's health, the history of care received, and how insurance and medical bills are paid, which makes them especially data-rich and very lucrative to cybercriminals.

In the US, patient data moves through 16 EHR platforms, and 571,045 providers who are affiliated with 4,023 different hospitals. According to the Healthcare Information and Management Systems Society (HIMSS), the average hospital has 16 different EMR vendors, and 75 percent of hospitals deal with 10 or more different outpatient vendors.[120]

The interconnected nature of these systems provides a level of convenience for all parties and supports various initiatives; however, it also presents cybercriminals with multiple avenues for gaining illegal access and pivoting into shared environments. Compromised patient data can be leveraged by criminals to fabricate false personas, file fake insurance claims, and potentially use the data to extort comprised individuals or entities.

Data breaches potentially cost the healthcare industry about $6.4 billion in 2018[v 121, 122, 123]

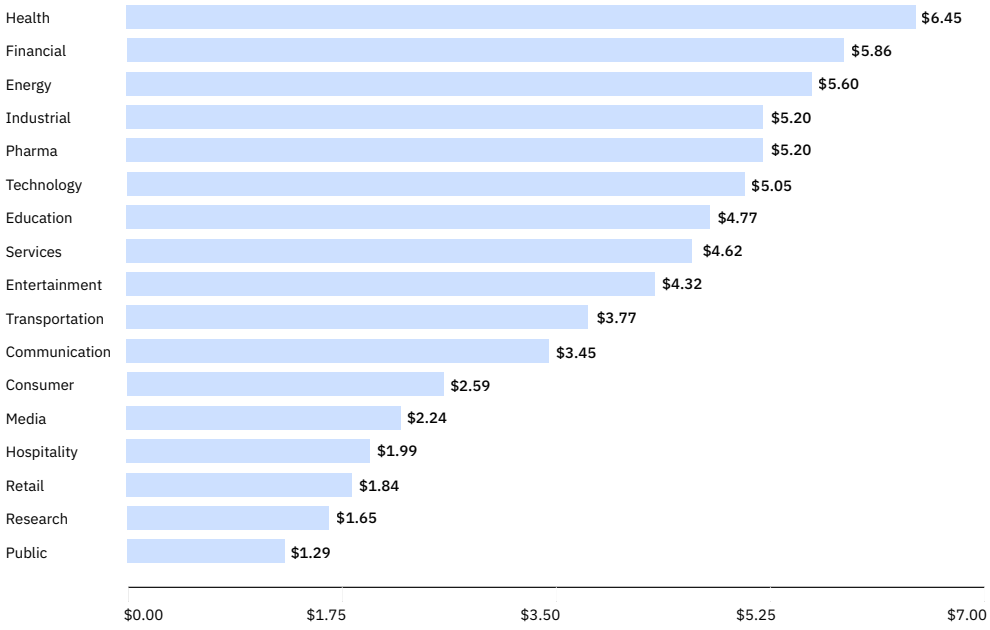

Figure 3: Average total cost per data breach by industry sector in US$ millions[124]

One of the key drivers of change in healthcare systems is the accelerated integration of existing systems and applications into the Internet of Things (IoT) infrastructure and cloud-based technologies.[125] Connected medical devices present potential vulnerabilities, as several outdated and legacy systems lack basic security features and may operate with unpatched software.

Given current activity trends and the amount of PII and PHI data collected, stored and shared by this sector, malicious cyber actors will continue to launch attacks on the healthcare infrastructure to steal data or disrupt operations as a means of extortion.

The healthcare sector is subject to a variety of regulatory and compliance requirements, but these requirements don't assure its ability to thwart today's sophisticated cyber threats without a thorough review of its present day, and future attack surface.

Guaranteeing patient safety and operational continuity likely requires the collaboration of government and the private sector to establish customized security frameworks and ensure adherence to relevant standards.[126]

March 2018 - July 2018:

In March, 2018, Minnesota Department of Human Services (DHS) experienced a compromise potentially exposing the PII of 10,263 individuals.[127] In June and July 2018, two separate phishing emails were sent to DHS employees containing a malicious link. Recipients who browsed to that link potentially provided malicious actors with access to employee email accounts and exposed the PHI of 20,800 people.[128]

April 2018:

An employee of Nemadji Research Corporation, a Los Angeles County DHS contractor, received a phishing email subsequently granting an attacker account access. As a result, Nemadji Research Corporation sent out a notification stating that the personal information of 14,591 DHS patients was potentially breached.[129]

June 2018:

The Alaska Department of Health and Social Services (DHSS) issued a statement regarding the compromise of a computer within the state's Division of Public Assistance network. The computer housed PHI and documents related to the status of pregnancy, death and incarceration, as well as Medicaid and Medicare billing codes, social security numbers, driver's license numbers, and other information, resulting in unauthorized access to the information of 87,000 Alaskans who received notification letters from the DHSS.[130] The department stated that the compromised system accessed sites in Russia and had a powerful information stealer, the Zeus Trojan, otherwise known as the Zbot Trojan, installed on it.[131]

January 2019:

Oregon Department of Human Services (DHS) suffered a cyber breach that started with a phishing email sent to nine department employees and contained a malicious link. The employees clicked on the link, reached a phishing site, and unwittingly gave account access to the attackers. Although the Enterprise Security Office team contained the incident, Oregon DHS sent out 645,000 breach notification letters and spent $485,000 to hire experts to investigate the incident. Possible PII involved included names, addresses and social security numbers.[132]

[v] According to a study published in the Health Insurance Portability and Accountability Act (HIPPA) Journal, the number of healthcare data breaches in 2018 resulted in the exposure of about 15 million records, tripling from the previous year. If you multiply the total amount of records lost by the estimated per capital cost of $429, per the 2019 Ponemon Institute Cost of a Data Breach report, the potential cost could amount to an approximate cost of $6.4 billion.

Please note: Estimates generated by X-Force IRIS are derived by multiplying the average cost per record lost by industry as prescribed by annual Cost of a Data Breach reports issued by the Ponemon Institute, and don't reflect the exact methodology developed by the Ponemon Institute. Exact figures may be lower for some breaches, which may have occurred prior to the publication of Ponemon's findings. Also, Ponemon's estimates don't include breaches in which more than 100,000 records were compromised, which may result in lower, actual costs per record. For further details on Ponemon's costing methodology, known as activity-based costing (ABC), please visit https://databreachcalculator.mybluemix.net/how-we-calculate-the-cost.

Election security

Participating in elections is a constitutional right for American citizens and the cornerstone of American democracy. There's a fundamental link between the security of election infrastructure and the confidence the public places in the outcome of digitally facilitated elections. Technological advancements in election functions can serve to increase participation and accessibility, but at the same time, inherent risks associated with the open nature of connected devices can provide an attractive target for malicious actors.[133]

Among the most sensitive systems supporting election security, voter registration databases (VRDBs) have been subject to the greatest targeting activity. VRDBs are not uniformly used or maintained across the country, and each may contain a variety of details about eligible electors. According to a 2019 US government report, foreign actors targeted VRDBs in at least seven states, either directly or through shared connections to other government databases or electoral equipment. While those compromised systems showed no evidence of tampering, data obtained in these attacks could be leveraged in future operations.[134]

State and local governments are responsible for protecting and conducting secure election processes. Each state, city and county may use a variety of different platforms, systems, methods, and processes for managing elections.[135] While it could be argued that the proliferation of disparate systems presents an inadvertent defense against large-scale attacks by avoiding the creation of a single point of failure, it also potentially presents threat actors with a variety of points of entry for conducting malicious activity.

The Brennan Center for Justice estimates that 16 million Americans will vote on paperless systems in the coming 2020 election, without a voter-verified paper ensuring authenticity. Digital ballots will be cast in many locations using legacy systems, running on hardware no longer produced—with election officials turning to eBay for replacement parts—and software no longer serviceable or able to receive patches for known vulnerabilities.[136] These conditions can only exacerbate the risk and vulnerability of an infrastructure that can't securely support its purpose.

The integrity of US elections has been making headlines since the US Central Intelligence Agency (CIA), National Security Agency (NSA) and FBI jointly stated with high confidence that the Russian government conducted a sophisticated interference campaign to influence American elections.[137] Russian state-sponsored cyber threat actors likely targeted state and local election-related systems in all 50 states to interfere with the US 2016 election cycle.[138, 139] While the reported type of activity included a range of vectors, the integrity of the election, or at least the vote count, didn't appear to be impacted according to investigators.[140]

The United States Senate Judiciary Committee's Subcommittee on Crime and Terrorism released a 2019 bipartisan report detailing Russia's use of social media as part of its election interference campaign. The Committee found that 50,258 automated Twitter accounts associated with the Russian state-supported Internet Research Agency (IRA) generated 2.12 million election-related Tweets, collectively receiving 457.7 million impressions within the first seven days of posting. The accounts impersonated news outlets, members of activist organizations, and politically engaged Americans in an attempt to sway the public to benefit Russia's political interests.[141]

March 2018:

The US president signed the Consolidated Appropriations Act, which included $380 million in grants for US states, with the goal "to enhance technology and make certain election security improvements," under the Help Americans Vote Act (HAVA).[142, 143, 144]

According to this act, states must match up to five percent of the federal funds they receive. As of April 2019, states have reportedly spent $108.12 million of the $380 million allocated for this purpose.[145] As of August 2019, reports indicate that states have spent the funds on training and hiring cybersecurity personnel to support election security, deploying end-point-detection solutions and replacing touchscreen balloting systems.[146] However, the results of a 2019 survey conducted by the Brennan Center for Justice, concluded that 31 states still needed to replace their equipment before the 2020 elections, two-thirds of which were found to be lacking adequate funds.[147]

July 2018:

According to the cochair of the Arizona Cybersecurity Team, the Arizona Secretary of State's office, which houses the electoral division, receives at least 50,000 intrusion attempts a month. The frequency of cyberattacks was brought to light following the FBI notification of an electoral-related breach during the 2016 general elections. A compromise of this network infrastructure could lead to the illegal access of sensitive voter information.[148]

October 2018:

Researchers discovered 35 million voter registration records from 19 states available for illegal sale on a hacking forum hosted on the dark web. The exposed data included citizens' PII and voter history. Voter records combined with other breached data could be used to disrupt election processes in addition to large-scale identity theft.[149] In 2015, the records of 191 million voters were exposed to the internet in a misconfigured database that didn't appear to have an owner.[150]

August and September 2019:

A threat group tracked by X-Force IRIS, Hive0003, which shares overlap with Phosphorus, made over 2,700 attempts to identify consumer email accounts and attacked 241 targeted accounts linked with the 2020 elections. While Hive0003 gained illegal access to four accounts, none of the accounts were associated with current or former US government officials, or any presidential campaign.[153]

August 2019:

Election security experts discovered the Vermont voting machine, AccuVote, could be accessed and subject to manipulation by malicious outsiders. At the DEF CON hacking convention,[154] ethical hackers tried to access similar voting machines known to be used by 135 towns in Vermont and found that they could manipulate the vote count results. The good news is, to corrupt and manipulate the votes on an AccuVote machine, a malicious actor would need to have physical access to the machine, limiting the ability of remote attackers to reach it.[155]

August 2019:

Election security experts also discovered that almost 36 backend election systems were connected to the internet over the last year, all while US election officials have stated that critical election systems are never connected to the internet and can't be hacked. Systems connected to the internet were found in 10 states, including election systems in nine Wisconsin counties, four Michigan counties and seven Florida counties.[156] Any connection to the internet increases the potential of remote attackers eventually finding a way to access these machines and possibly attacking them to affect the integrity of their data output.

In many types of voting equipment, the votes are typically stored inside the machines on a memory card that is then collected and driven by poll workers to county election offices after polls close. However, some counties transmit the votes electronically to expedite the process. The system receiving the electronically transmitted results is an secure file transfer protocol (SFTP) server connected to the internet behind a firewall. To minimize the potential of unauthorized access, the server and firewall should only be connected to the internet for a few moments before an election, and just long enough afterwards to receive all the votes. However, researchers have observed that some of these systems remain connected to the internet for months or even year-round, creating a vastly vulnerable target for hackers.[157]

October 2019:

According to West Virginian state officials, hacking attempts were made upon the state's out-of-state voter's mobile application, Voatz, during the 2018 election cycle. While there was no impact to the 144 ballots cast, federal investigators are currently looking into the possibility of the alleged intrusion attempts being the result of testing by computer science students at the University of Michigan, and not by malicious actors. The University of Michigan is one of the few American universities featuring a curriculum focused on election security.[151, 152]

Focus on preparedness, bolster resilience

Focus on preparedness and bolster resilience

Know your environment and establish requirements

Many states are developing informed responses to cyber threats, modifying their infrastructures by evaluating their environments and applicable risks, and allocating necessary resources to address issues and critical requirements.

At the federal level, the national government is introducing and adopting new legislation to bolster the resources and protections available to local governments. In late October 2019, the bipartisan DOTGOV Online Trust in Government Act was introduced to the US Senate. Intended to strengthen cybersecurity at the local government level, the bill would enable local governments to migrate infrastructure to secure, federally administered .gov internet domains. For those local governments that choose to make the switch, the bill guarantees resources and support from the United States Department of Homeland Security (DHS).[162] This proposal follows the passing of the DHS Cyber Hunt and Incident Response Teams Act of 2019, which authorizes the DHS to maintain and deploy incident response and cyber hunt teams to help government and private sector entities recover from a malicious cyber event.[163]

2015:

The governor of California signed Executive Order B-34-15, which created the California Cyber Security Integration Center (Cal-CSIC). The Cal-CSIC's mission is "to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state." Cal-CSIC serves as the central hub for cybersecurity activities within the state and coordinates information sharing with local, tribal, non-governmental organizations (NGOs), academic institutions, federal agencies and other service providers.[158]

January 2017:

The Georgia governor released budget recommendations to the General Assembly, which prioritized cybersecurity, education, public safety, healthcare, economic development, and efficiency in government procedures. Highlighting the importance of cybersecurity, the budget includes a $50 million budget allocation for a new Georgia Cyber Innovation and Training Center in partnership with state and federal agencies, and private sector companies.[159]

January 2018:

Santa Clara County, California is taking significant steps to harden the county's network infrastructure. It's modernizing the county's IT infrastructure by merging its hospital and social services systems, and redesigning and updating IT job descriptions to accurately capture pertinent roles that attract qualified candidates. The county is also upgrading its public safety and criminal justice systems by replacing 1990s-era mainframes and implementing connections across all agencies to maintain access, data privacy and a secure data-sharing environment.[160]

January 2018:

Ohio is also edging towards resilience as the Ohio Department of Administrative Services (DAS) moves to implement a new program to improve statewide cybersecurity, engaging with local governments and school districts. The program aims to instill best practices and help entities tap into requisite financial resources. Arkansas, Guam, Louisiana, Maryland, Massachusetts, and Washington are also among those states and territories selected by the National Governors Association to participate in this partnership.[161]

Understanding the threat landscape and acting on intelligence

State and local governments provide a remarkable variety of services to constituents and must consistently defend a vast amount of systems. To establish effective protections for any environment, defenders must understand the threats they face. To act on accurate and actionable information, one best practice is to have access to and consult reliable and well-informed threat intelligence. Local governments can benefit from actionable insight into active threats to determine their jurisdiction's risk level, and budget accordingly to develop appropriate means of response.

Connect and collaborate to share information

Cyberattacks on critical systems are of equal concern to public and private sector entities that jointly look to shield their networks, data, and users from malicious activity. To gain an accurate picture of the operational environment, all parties need to share their unique perspectives of threat activity to develop greater collective visibility.

To facilitate this effort, several government and private sector groups have developed Information Sharing and Analysis Centers, commonly known as ISACs. These nonprofit organizations provide a secure environment to support two-way sharing between ISAC members on the latest threat activities, trends, and best practices.

A Cyber threat intelligence sharing platform (TISP)

Creating a sharing platform at the local, city, and state levels can furnish the business, utilities, financial, healthcare, entertainment, and critical infrastructure sectors with up-to-date threat intelligence. The IBM Security X-Force LA Cyber Lab™ TISP enables citizens to educate themselves on the latest business email compromises and ransomware campaigns. Enriched with data from partners[165] like IBM X-Force IRIS, trends and events can be correlated with data on prominent threat group activity.

Systematic simulation

It's not enough to have a disaster recovery plan on hand and hope for the best. Fortune favors the prepared. From fire drills to war gaming, professionals practice their response to disaster so that when the smoke—or digital dust—is in the sky, those in their charge walk away unscathed. Learn more about IBM Security Command Centers, designed to help teams prepare for attacks with real-time breach simulations and response training.

Complimentary cyber range training for cities

Developed to train cities on incident response and preparedness through cyberattack simulations and created specifically for the public sector, these custom simulations take place once a month, immersing attendees in what it would be like to experience a cyberattack attack against their city.

The IBM Security Command Center, a full-scale cyber range in Cambridge, Massachusetts, immerses attendees in simulated cyberattacks to train them on how they can prepare for, respond to, and manage a broad variety of threats under fire, so to speak. Simulations use live malware, ransomware and other real-world hacker tools to deliver realistic cyberattack experiences. The facility features a fully operational air-gapped network of a fictitious entity used for simulated attacks.

Since opening its doors in November 2016, the IBM Security Command Center has hosted more than 4,500 visitor organizations, including major banks, retailers, hospitals, law enforcement and government representatives.[166]

Learn more about the IBM Security Command Center at **ibm.com/xforcecommand.**

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
December 2019

[1] "Local government cybersecurity practices." *ICMA.* https://icma.org/sites/default/files/19-053%20Survey%20Research%20Snapshots_Cybersecurity_web.pdf

[2] "Local government cybersecurity practices." *ICMA.* https://icma.org/sites/default/files/19-053%20Survey%20Research%20Snapshots_Cybersecurity_web.pdf

[3] Brendan I. Koerner. "Inside the Cyberattack That Shocked the US Government." *Wired*, October 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

[4] Larry Ponemon. "What's New in the 2019 Cost of Data Breach Report." *Security Intelligence*, July 23, 2019. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[5] Consumers at risk: 126% increase in exposed consumer data, 1.68 billion email-related credentials." *Identity Theft Resource Center,* January 28, 2019. https://www.idtheftcenter.org/tag/2018-annual-data-breach-report/

[6] "Federal Cybersecurity: American's Data at Risk." *United States Senate*. https://www.portman.senate.gov/sites/default/files/2019-06/2019.06.25-PSI%20Report%20Final%20UPDATE.pdf

[7] "State CIO Top 10 Priorities." *NASCIO.* https://www.nascio.org/Portals/0/Publications/Documents/2019/NASCIO_Top10_lettersize.pdf

[8] Larry Ponemon. "What's New in the 2019 Cost of Data Breach Report." *Security Intelligence*, July 23, 2019. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[9] Allan Liska. "Early Findings: Review of State and Local Government Ransomware Attacks." *Recorded Future.* https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf

[10] Jeff Ostrowski and Tony Doris. "How a Riviera Beach police department email that shouldn't have been opened turned disastrous for the city." *The Palm Beach Post,* June 7, 2019. https://www.palmbeachpost.com/news/20190607/how-riviera-beach-police-department-email-that-shouldnt-have-been-opened-turned-disastrous-for-city

[11] The 2018 State CIO Survey." *NASCIO, Grant Thorton LLP and CompTIA,* October 2018. https://www.nascio.org/Portals/0/Publications/Documents/2018/2018StateCIOSurvey.pdf

[12] "Digital Transformation for Local Governments." *ICMA and OnBase by Hyland*, October 2018. https://icma.org/sites/default/files/ICMA%20Digital%20Transformation%20White%20Paper_final_0.pdf

[13] Dave Orrick. "Facing 3 million digital attacks daily, Minnesota government plans increased security." *St. Paul Pioneer Press,* April 13, 2018. https://www.duluthnewstribune.com/news/4431798-facing-3-million-digital-attacks-daily-minnesota-government

[14] "Local government cybersecurity practices." *ICMA.* https://icma.org/sites/default/files/19-053%20Survey%20Research%20Snapshots_Cybersecurity_web.pdf

[15] "Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher." *(ISC)²*, June 7, 2017. https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage

[16] Danny Palmer. "WannaCry ransomware: Hospitals were warned to patch system to protect against cyber-attack – but didn't." *ZDNet,* October 27, 2017. https://www.zdnet.com/article/wannacry-ransomware-hospitals-were-warned-to-patch-system-to-protect-against-cyber-attack-but-didnt/

[17] Darlene Storm. "Police lost 8 years of evidence in ransomware attack." *Computer World,* January 30, 2017. https://www.computerworld.com/article/3163046/police-lost-8-years-of-evidence-in-ransomware-attack.html

[18] Jacob Poushter and Janell Fetterolf. "International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security." *Pew Research Center,* January 9, 2019. https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/

[19] "Potential Cost of a Data Breach SEMA4." *Minnesota Government*. https://mn.gov/mnit/assets/data-breach-cost-infographic_tcm38-335672.pdf

[20] Dave Orrick. "Facing 3 million digital attacks daily, Minnesota government plans increased security." *Duluth News Tribune.* April 13, 2018. https://www.duluthnewstribune.com/news/4431798-facing-3-million-digital-attacks-daily-minnesota-government

[21] Heather Kuldell. "10 Government Legacy Systems Cost Taxpayers $337 Million Every Year." *Nextgov,* June 12, 2019.https://www.nextgov.com/it-modernization/2019/06/10-government-legacy-systems-cost-taxpayers-337-million-every-year/157682/

[22] "All State of Hawai'i Employees Now on New Revolutionary Payroll System." *State of Hawaii.* https://ags.hawaii.gov/hip/news-releases/all-state-of-hawai%CA%BBi-employees-now-on-new-revolutionary-payroll-system/

[23] Bradley Barth. "Hundreds of Delaware residents among the victims of BenefitMall breach." *SC Magazine*, January 29, 2019. https://www.scmagazine.com/home/security-news/data-breach/hundreds-of-delaware-residents-among-the-victims-of-benefitmall-breach/

[24] Jessica Davis. "4-Month Breach of BenefitMall Impacts 112,000 Plan Members." *Health IT Security*, January 15,

2019. https://healthitsecurity.com/news/4-month-breach-of-benefitmall-impacts-112000-plan-members

[25] John Dunn. "Is Payroll The Weak Link In Your Organization's Cybersecurity Network?" *Tech Times,* May 14, 2019. https://www.techtimes.com/articles/243170/20190514/is-payroll-the-weak-link-in-your-organizations cybersecurity-network.htm

[26] Karl Etters. "Almost $500,000 swiped in city of Tallahassee payroll hack." *Tallahassee Democrat,* April 5, 2019. https://www.tallahassee.com/story/news/2019/04/05/almost-500-k-swiped-city-tallahassee-payroll-hack/3379242002/

[27] "Testimony of Assistant Secretary Karen S. Evans." *Office of Cybersecurity, Energy Security, and Emergency Response. US Department of Energy Before the Committee on Energy & Natural Resources. United States Senate,* February 14, 2019. https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=03BA54D2-A59B-43F8-A26D-CD027E675022

[28] "National Cyber Strategy of the United States of America." *The President of the United States of America,* September 2018. https://fas.org/irp/eprint/cyber-strat.pdf

[29] Jacob Poushter and Janell Fetterolf. "International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security." *Pew Research Center.* January 9, 2019. https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/

[30] Thomas Brewster. "Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System." *Forbes,* November 28, 2016. https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/#1564349e4706

[31] Joey Cresta. "Virus attacks Greenland Town Hall computers." *Seacoast Online,* January 2, 2014. https://www.seacoastonline.com/article/20140102/NEWS/401020387

[32] Allan Liska. "Early Findings: Review of State and Local Government Ransomware Attacks." *Recorded Future.* https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf

[33] "TET 2018 – Chapter 2 – Transportation's Contribution to the Economy." *United States Department of Transportation,* December 18, 2018. https://www.bts.gov/transportation-economic-trends/tet-2018-chapter-2-contribution-economy

[34] Claudia Geib. "Hackers Are Holding The City of Atlanta Hostage." *Futurism,* March 27, 2018. https://futurism.com/atlanta-hacking-ransomware-cybersecurity

[35] Mathew J. Schwartz. "Ransomware Result: Free Ticket to Ride in San Francisco." *Bank Info Security,* November 28, 2016. http://www.bankinfosecurity.com/ransomware-result-free-ticket-to-ride-in-san-francisco-a-9562

[36] "Sacramento Regional Transit Systems Hit By Hacker." *CBS Sacramento*, November 20, 2017. https://sacramento.cbslocal.com/2017/11/20/sacramento-regional-transit-systems-hit-by-hacker/

[37] Jacob Poushter and Janell Fetterolf. "International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security." *Pew Research Center.* January 9, 2019. https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/

[38] "Potential Cost of a Data Breach SEMA4." *Minnesota Government*. https://mn.gov/mnit/assets/data-breach-cost-infographic_tcm38-335672.pdf

[39] Dave Orrick. "Facing 3 million digital attacks daily, Minnesota government plans increased security." *Duluth News Tribune.* April 13, 2018. https://www.duluthnewstribune.com/news/4431798-facing-3-million-digital-attacks-daily-minnesota-government

[40] Heather Kuldell. "10 Government Legacy Systems Cost Taxpayers $337 Million Every Year." *Nextgov.* June 12, 2019. https://www.nextgov.com/it-modernization/2019/06/10-government-legacy-systems-cost-taxpayers-337-million-every-year/1 57682/

[41] "Electric Grid Cybersecurity." *Congressional Research Service.* September 4, 2018. https://fas.org/sgp/crs/homesec/R45312.pdf

[42] "All State of Hawai'I employees now on new revolutionary payroll system." *State of Hawaii.* https://ags.hawaii.gov/hip/news-releases/all-state-of-hawai%CA%BBi-employees-now-on-new-revolutionary-payroll-system/

[43] "Smart Cities Market Size Worth $237.6 Billion by 2025." *Grand View Research,* May 2019. https://www.grandviewresearch.com/press-release/global-smart-cities-market

[44] Luther Turmelle. "Survey Highlights Utility Cyber Insecurities." *New Haven Register,* December 17, 2018. https://www.govtech.com/security/Survey-Highlights-Utility-Cyber-Insecurities.html

[45] Claire Zaboeva. "Why You Should Practice and Drill to Prepare for a Cyber Emergency." *Security Intelligence,* October 17, 2018. https://securityintelligence.com/why-you-should-practice-and-drill-to-prepare-for-a-cyber-emergency/

[46] Mark Feuerborn. "10,000 Topekans potentially hit in cyber-attack on city utilities website." *KSNT,* December 10, 2018. https://www.ksnt.com/news/10000-topekans-potentially-hit-in-cyber-attack-on-city-utilities-website/

[47] Bradley Barth. "Click2Gov breach threatens credit card data of Hanover County residents." *SC Magazine,* January 16, 2019. https://www.scmagazine.com/home/security-

news/click2gov-breach-threatens-credit-card-data-of-hanover-county-residents/

[48] Dan Goodin. "Hackers Hit Click2Gov Bill-Paying Portals in 8 Cities." *Wired.* September 21, 2019. https://www.wired.com/story/hackers-hit-click2gov-bill-paying-portals/

[49] "Murfreesboro Water Department's bill pay website hacked." *NewsChannel5 Nashville*, August 3, 2019. https://www.newschannel5.com/news/murfreesboro-water-departments-bill-pay-website-hacked

[50] "Consumers at risk: 126% Increase in Exposed Consumer Data, 1.68 Billion Email-Related Credentials." *Identity Theft Resource Center*, January 28, 2019. https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/

[51] "Moore Announces Formation of Data Security Working Group." *Oklahoma State Legislature.* https://www.okhouse.gov/Members/ShowStory.aspx?MediaNewsID=5346&rwndrnd=0.415887045674026

[52]Jim Rosica. "State investigating 'possible' criminal breach of driver's license info." *Florida Politics,* June 16, 2018. https://floridapolitics.com/archives/266431-driver-license-data-breach

[53] Patrick May. "It's not the DMV! Bogus websites take advantage of agency's woes." *Bay Area News Group,* October 2, 2018. https://www.mercurynews.com/2018/10/02/its-not-the-dmv-bogus-websites-take-advantage-of-agencys-woes/

[54] "PennDOT issues warning about fake DMV websites." *11 News WPXI,* December 4, 2018. https://www.wpxi.com/news/top-stories/penndot-issues-warning-about-fake-dmv-websites/883361836

[55] Christopher Magan. "MNLARS has another hiccup; 1,500 motorists' private data shared." *Pioneer Press,* January 3, 2019. https://www.twincities.com/2019/01/03/dmv-mnlars-has-another-hiccup-1500-motorists-private-data-shared

[56] Ashlynn Worley. "El Paso County Clerk's Office warns of DMV website scams." *KOAA News5,* March 11, 2019. https://koaa.com/news/covering-colorado/2019/03/11/el-paso-county-clerks-office-warn-of-dmv-website-scams/

[57] Tina Sfondeles. "All clear? Server exposure from Illinois vendor with access to driver's license data raises questions." *Chicago Sun Times,* July 22, 2019. https://chicago.suntimes.com/politics/2019/7/22/20700016 /server-exposure-illinois-chicago-vendor-drivers-license-data-jesse-white-anna-valencia

[58] Renu Bhatia. "Biometrics and Face Recognition Techniques." *International Journal of Advanced Research in Computer Science and Software Engineering,* May 2013. https://pdfs.semanticscholar.org/a7cf/ede8225c99f6e1883d4ae14c66fb20191117.pdf

[59] Molly Ramsdell. "Real ID is for Real." *National Conference of State Legislatures,* March 2014. http://www.ncsl.org/research/transportation/real-id-is-for-real.aspx

[60] "Fingerprints and Other Biometrics." *FBI.* https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics

[61] Mariella Moon. "FBI nabs Chinese national linked to massive OPM hack." *Engadget*, August 25, 2017. https://www.engadget.com/2017/08/25/fbi-nabs-chinese-national-opm-hack/

[62] Elaine S. Povich. "Real ID, real problems: States cope with changing rules, late rollouts." *GCN,* August 8, 2019. https://gcn.com/articles/2019/08/08/real-id.aspx

[63] Jon Porter. "Huge security flaw exposes biometric data of more than a million users." *The Verge,* August 14, 2019. https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data/

[64] Sasha Romanosky, Karlyn D. Stanley, Jirka Taylor and Zev Winkelman. "Law Enforcement Cyber Center Final Technical Report." *RAND Corporation.* https://www.rand.org/pubs/research_reports/RR2320.html

[65] "The Cost of Malicious Cyber Activity to the U.S. Economy." *The Council of Economic Advisers,* February 2018. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[66] "2018 Internet Crime Report." *Federal Bureau of Investigation Internet Crime Complaint Center.* https://pdf.ic3.gov/2018_IC3Report.pdf

[67] "National Crime Information Center (NCIC)." *FBI.* https://www.fbi.gov/services/cjis/ncic

[68] Jason Aycock. "AT&T updates on FirstNet buildout." *Seeking Alpha,* August 12, 2019. https://seekingalpha.com/news/3490728-t-updates-firstnet-buildout

[69]Michael J.D. Vermeer, Dulani Woods and Brian A. Jackson. "Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers." *RAND Corporation.* https://www.rand.org/pubs/research_reports/RR2240.html

[70] Stephanie Kanowitz. "Is FirstNet secure enough for law enforcement?" *GCN,* March 6, 2018. https://gcn.com/articles/2018/03/06/firstnet-cjis.aspx

[71] "Notice of Data Privacy Incident." *Township of Maplewood, New Jersey,* August 7, 2019. https://www.twp.maplewood.nj.us/home/news/notice-data-privacy-incident

[72] Zack Whittaker. "Hackers publish personal data on thousands of US police officers and federal agents." *TechCrunch,* April 12, 2019. https://techcrunch.com/2019/04/12/police-data-hack/

[73] Jeff Ostrowski. "How a Riviera Beach police department email that shouldn't have been opened turned disastrous for the city." *The Palm Beach Post.* June 7, 2019.

https://www.palmbeachpost.com/news/20190607/how-riviera-beach-police-department-email-that-shouldnt-have-been-opened-turned-disastrous-for-city

[74] Eric Leonard, Phil Drechsler and Andrew Blankstein. "LAPD Police Officers' Personal Information Stolen in Data Breach." *NBC Los Angeles,* July 29, 2019. https://www.nbclosangeles.com/news/local/LAPD-Police-Officers-Personal-Information-Stolen-Data-Breach-513340401.html

[75] Benjamin Freed. "Hackers took $4.2 million from pension fund for Oklahoma troopers." *State Scoop*, September 9, 2019. https://statescoop.com/hackers-took-4-2-million-pension-fund-oklahoma-troopers/

[76] Nolan Clay. "Hackers get $4.2 million from Oklahoma pension fund for retired troopers, state agents." *The Oklahoman,* September 6, 2019. https://oklahoman.com/article/5640503/hackers-get-42-million-from-pension-fund-for-retired-troopers-state-agents

[77]Benjamin Freed. "Hackers took $4.2 million from pension fund for Oklahoma troopers." *State Scoop*. September 9, 2019. https://statescoop.com/hackers-took-4-2-million-pension-fund-oklahoma-troopers/

[78] William Petroski. "IPERS' pension accounts compromised in cybercrime scam." *Des Moines Register*, November 1, 2017. https://www.desmoinesregister.com/story/news/2017/11/01/ipers-pension-accounts-compromised-fbi-asked-investigate/823078001/

[79] Ben Evarts and Gary Stein. "U.S. Fire Department Profile 2017." *National Fire Protection Association,* March 2019. https://www.nfpa.org/-/media/Files/News-and-Research/Fire-statistics-and-reports/Emergency-responders/osfdprofile.pdf

[80] Annie Kitch. "Deploying next generation 911." *National Conference of State Legislatures.* Volume 27, Number 10, March 2019. http://www.ncsl.org/research/telecommunications-and-information-technology/deploying-next-generation-911.aspx

[81] Tanya Mohn. "911 Gets an Upgrade; Millions In Grants Aim To Boost Public Safety By Modernizing Systems." *Forbes,* August 18, 2019. https://www.forbes.com/sites/tanyamohn/2019/08/18/911-gets-an-upgrade-millions-in-grants-aim-to-boost-public-safety-by-modernizing-systems/#7baf288d6d1d

[82]"A Guide for State & Local Authorities." *NG911 & FirstNet*. https://www.911.gov/pdf/NASNA_National_911_Program_NG911_FirstNet_Guide_State_Local_Authorities.pdf

[83] "NG-911, Inc. Integrates the Industry's Best Subcontractors." *NG-911, Inc.* http://www.ng-911inc.com/index.php?option=com_content&view=article&id=72&Itemid=475

[84] "Cyber Risks to Next Generation 9-1-1." *Office of Emergency Communications*. November 2018. https://www.911.gov/pdf/OEC_Cyber_Risks_to_NG911_November_2018.pdf

[85] "Foreign Economic Espionage in Cyberspace 2018." *National Counterintelligence and Security Center.* https://www.dni.gov/files/NCSC/documents/supplychain/20190327-economic-espionage-pub02.pdf

[86] "Baltimore's 911 emergency system hit by cyberattack." *Reuters,* March 28, 2018. https://www.nbcnews.com/news/us-news/baltimore-s-911-emergency-system-hit-cyberattack-n860876

[87] Jon Schuppe. "Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?" *NBC News,* April 3, 2018. https://www.nbcnews.com/news/us-news/hackers-have-taken-down-dozens-911-centers-why-it-so-n862206 [88] "Ransomware Attack Wipes Out Police and Fire Department Data." *HackRead,* May 13, 2018. https://www.hackread.com/ransomware-attack-wipes-out-police-fire-department-data/

[89] "FDNY Sends Notices to 10,000 Individuals Concerning Possible Data Breach." *Fire Department City of New York,* August 9, 2019. https://www1.nyc.gov/site/fdny/news/fa5719/fdny-sends-notices-10-000-individuals-concerning-possible-data-breach#/0

[90] "The Federal Role in Education." *U.S. Department of Education*, May 25, 2017. https://www2.ed.gov/about/overview/fed/role.html

[91] "Update Concerning China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation." *Office of the United States Trade Representative Executive Office of the President,* November 20, 2018. https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf

[92] "Doing Business with DOD." *U.S. Department of Defense.* https://dod.defense.gov/Resources/Contract-Resources/

[93] Larry Ponemon. "What's New in the 2019 Cost of Data Breach Report." *Security Intelligence*. July 23, 2019. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[94] Consumers at risk: 126% increase in exposed consumer data, 1.68 billion email-related credentials." *Identity Theft Resource Center.* January 28, 2019. https://www.idtheftcenter.org/tag/2018-annual-data-breach-report/

[95] "Data Breach Reports." *Identity Theft Resource Center,* August 31, 2019. https://www.idtheftcenter.org/wp-content/uploads/2019/09/2019-August-Data-Breach-Package-1.pdf

[96] Jessica Davis. "417,000 Augusta University Health patient records breached nearly one year ago." *Healthcare IT News*, August 17, 2018. https://www.healthcareitnews.com/news/417000-augusta-

university-health-patient-records-breached-nearly-one-year-ago

[97] "ITG09 Analysis Report." *X-Force IRIS*, July 14, 2019. https://exchange.xforce.ibmcloud.com/threat-group/03d5177b1b98ab20c420dc2203734b41

[98] Axel F and Pierre T. "Leviathan: Espionage actor spearphishes maritime and defense targets." *Proofpoint,* October 16, 2017. https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

[99] "Section 3: China's 13th Five-year Plan." 2016 Annual Report to Congress. *US-China Economic and Security Review Commission,* November 2016. https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%201%2C%20Section%203%20-%2013th%20Five-Year%20Plan.pdf

[100] "Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries." *FireEye,* March 16, 2018. https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

[101] "Leviathan: Espionage actor spearphishes maritime and defense targets." *ProofPoint.* October 16, 2017. https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

[102] Fred Plan, Nalani Fraser, Jacqueline O'Leary, Vincent Cannon and Ben Read. "APT 40: Examining a China-Nexus Espionage Actor." *FireEye*, March 4, 2019. https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

[103] "Leviathan: Espionage actor spearphishes maritime and defense targets." *ProofPoint.* October 16, 2017. https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

[104] "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps." *United States Department of Justice. US Attorney's Office. Southern District of New York*, March 23, 2018. https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic

[105] "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps." Department of Justice. US Attorney's Office. Southern District of New York. Friday March 23, 2018. https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic

[106] "Iranian Mabna Hackers." *FBI*, March 23, 2018. https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers

[107] Counter Threat Unit Research Team. "COBALT DICKENS Goes Back to School… Again." *Secureworks,* September 11, 2019. https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again

[108] "417,000 Individuals Affected by Augusta University Health Phishing Attack." *HIPAA Journal*, August 17, 2018. https://www.hipaajournal.com/417000-individuals-affected-by-augusta-university-health-phishing-attack/

[109] Web Staff. "Chesapeake Public Schools' computer network affected by malware from phishing emails." *WTKR,* November 8, 2019. https://wtkr.com/2018/11/08/chesapeake-public-schools-computer-network-affected-by-malware-from-phishing-emails/

[110] Eric Stirgus. "Georgia Tech mistakenly releases data about nearly 8,000 students." *The Atlanta Journal-Constitution,* July 27, 2019. https://www.ajc.com/news/local-education/georgia-tech-mistakenly-releases-data-about-nearly-000-students/s0qiPCNY2OeUiAPyctO0OP/#

[111] Aaron Diamant. "Georgia Tech says data breach exposed info of 1.3 million people." *WSB-TV Atlanta,* April 2, 2019. https://www.wsbtv.com/news/local/georgia-tech-says-data-breach-exposes-information-from-13-million-people/936316583

[112] Joseph C. Chen. "Mirrorthief Group Uses Magecart Skimming Attack to Hit Hundreds of Campus Online Stores in US and Canada." *TrendMicro Security Intelligence Blog,* May 3, 2019. https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/

[113] Jayed Rahman. "Paterson: 23,000 school district passwords stolen in data breach." *Paterson Times,* May 13, 2019. http://patersontimes.com/2019/05/13/paterson-23000-school-district-passwords-stolen-in-data-breach/

[114] Melissa Topey. "School division announces third-party data breach." *The Northern Virginia Daily,* July 30, 2019. https://www.nvdaily.com/nvdaily/school-division-announces-third-party-data-breach/article_f392eb6e-048a-5400-81c6-0a196c849124.html

[115] "Personal Info Of 51,000 Students, Staff Involved In Indian Prairie School District Data Breach." *CBS Chicago,* August 6, 2019. https://chicago.cbslocal.com/2019/08/06/personal-info-of-51000-students-staff-involved-in-indian-prairie-school-district-data-breach/

[116] Addison School District 4. https://www.asd4.org/apps/news/article/1069304

[117] "Medicaid: An Overview." *Congressional Research Service,* June 24, 2019. https://crsreports.congress.gov/product/pdf/R/R43357

[118] "State Children's Health Insurance Program." *Benefits.gov*. https://www.benefits.gov/benefit/607

[119] "What are the differences between electronic medical records, electronic health records, and personal health records?" *HealthIT.gov.* https://www.healthit.gov/faq/what-are-differences-between-electronic-medical-records-electronic-health-records-and-personal

[120] Tom Sullivan. "Why EHR data interoperability is such a mess in 3 charts." *HealthcareIT News,* May 16, 2018. https://www.healthcareitnews.com/news/why-ehr-data-interoperability-such-mess-3-charts

[121] "2019 Data Breach Barometer Report Shows Massive Increase in Exposed Healthcare Records." *HIPAA Journal.* February 13, 2019. https://www.hipaajournal.com/2019-data-breach-barometer-report-shows-massive-increase-in-exposed-healthcare-records/

[122] "Enforcement Highlights." *U.S. Department of Health & Human Services,* October 31, 2019. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

[123] Larry Ponemon. "What's New in the 2019 Cost of Data Breach Report." *Security Intelligence*. July 23, 2019. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[124] Larry Ponemon. "What's New in the 2019 Cost of Data Breach Report." *Security Intelligence*. July 23, 2019. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[125] "US Healthcare Cybersecurity Market to Reach $8.70 Billion by 2023 as Companies Adopt IoT and Cloud Strategies." *Frost & Sullivan,* April 23, 2019. https://www.prnewswire.com/news-releases/us-healthcare-cybersecurity-market-to-reach-8-70-billion-by-2023-as-companies-adopt-iot-and-cloud-strategies-300836471.html

[126] CyberMDX Raises $10 Million Series A to Expand Medical Cybersecurity to Hospitals Worldwide." *Business Wire,* July 17, 2018. https://www.businesswire.com/news/home/20180717005094/en/CyberMDX-Raises-10-Million-Series-Expand-Medical

[127] Pierluigi Paganini. "Minnesota Department of Human Services announced to have suffered a data breach that may have exposed the personal information of about 11,000 people." *Security Affairs*, April 10, 2019. https://securityaffairs.co/wordpress/83609/data-breach/minnesota-department-of-human-services-breach.html

[128] "Minnesota DHS Notifies 21,000 Patients That Their PHI Has Potentially Been Compromised." *HIPAA Journal.* October 12, 2018. https://www.hipaajournal.com/minnesota-dhs-21000-patients-phishing-attack/

[129] "Data Breach Notification." *Nemadji.* July 8, 2019. http://file.lacounty.gov/SDSInter/dhs/1058017_NemadjiBreach-DHSSubstituteNoticeEnglish7-3-19.pdf#

[130] "State revises count of letters sent over security breach." *KTVA,* January 22, 2019. https://www.ktva.com/story/39834995/state-sends-at-least-500000-letters-over-security-breach

[131] "HIPAA and APIPA Breach Notification." *State of Alaska Department of Health & Social Services,* June 28, 2018. http://dhss.alaska.gov/News/Documents/press/2018/2018-HIPAA-Breach.pdf

[132] Stephen White. "DHS data breach hits 645,000 Oregon citizens in the US." *PrivSec Report.* June 19, 2019. https://gdpr.report/news/2019/06/19/dhs-data-breach-oregon/

[133] "Update on Results for Retrospective Review of Russian-Related Election Activity." *United States Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism,* January 19, 2019. https://www.judiciary.senate.gov/imo/media/doc/Edgett%20Appendix%20to%20Responses.pdf

[134] "Election Security: Voter Registration Systems Policy Issues." *Congressional Research Service,* August 7, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11285

[135] "Election Security: Federal Funding for Securing Election Systems." *Congressional Research Service,* August 8, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11286

[136] Lawrence Norden. "How to Secure Elections for 2020 and Beyond." *Brennan Center for Justice,* October 23, 2019. https://www.brennancenter.org/our-work/research-reports/how-secure-elections-2020-and-beyond

[137] "Assessing Russian Activities and Intentions in Recent US Elections." *Office of the Director of National Intelligence United States of America, National Intelligence Council*, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf

[138] "Election Security: Federal Funding for Securing Election Systems." *Congressional Research Service,* August 8, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11286

[139] "The Designation of Election Systems as Critical Infrastructure." *Congressional Research Service,* September 18, 2019. https://crsreports.congress.gov/product/pdf/IF/IF10677

[140] "The Designation of Election Systems as Critical Infrastructure." *Congressional Research Service,* September 18, 2019. https://crsreports.congress.gov/product/pdf/IF/IF10677

[141] "Update on Results for Retrospective Review of Russian-Related Election Activity." *United States Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism,* January 19, 2019. https://www.judiciary.senate.gov/imo/media/doc/Edgett%20Appendix%20to%20Responses.pdf

[142] Kim Zetter. "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials." *Vice,* August 8, 2019. https://www.vice.com/en_us/article/3kxzk9/exclusive-

critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

[143] "Election Security: Federal Funding for Securing Election Systems." *Congressional Research Service*, August 8, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11286

[144] Benjamin Freed. "Senate breakthrough on election security funding 'encouraging'." *StateScoop,* September 19, 2019. https://statescoop.com/senate-breakthrough-election-security-funding-encouraging/

[145] "Election Security: Federal Funding for Securing Election Systems." Congressional Research Service. August 8, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11286

[146] Benjamin Freed. "Congress moving closer toward cybersecurity aid to state and local governments." *StateScoop,* September 23, 2019. https://statescoop.com/congress-moving-closer-toward-cybersecurity-aid-to-state-and-local-governments/

[147] Lawrence Norden. "How to Secure Elections for 2020 and Beyond." *Brennan Center for Justice,* October 23, 2019. https://www.brennancenter.org/our-work/research-reports/how-secure-elections-2020-and-beyond

[148] Christopher Conover. "Hackers Take Aim at State, Including Elections, Millions of Times a Month." *Arizona Public Media*, July 13, 2018. https://www.azpm.org/p/azillhome/2018/7/13/133168-hackers-take-aim-at-state-including-elections-millions-of-times-a-month/

[149] Ms. Smith. "35 million voter records from 19 states for sale on hacking forum." *CSO Online,* October 16, 2018. https://www.csoonline.com/article/3313646/35-million-voter-records-from-19-states-for-sale-on-hacking-forum.html

[150] Steve Ragan. "Database configuration issues expose 191 million voter records." *CSO Online,* December 28, 2015. https://www.csoonline.com/article/3018592/database-configuration-issues-expose-191-million-voter-records.html

[151] Benjamin Freed. "Alleged mobile voting app hack linked to University of Michigan." *StateScoop,* October 7, 2019. https://statescoop.com/alleged-mobile-voting-app-hack-linked-university-michigan-report/

[152] Benjamin Freed. "Hacking attempt reported against West Virginia's mobile voting app." *StateScoop,* October 2, 2019. https://statescoop.com/voatz-voting-app-west-virginia-fbi-hacking-attempt/

[153] Tom Burt. "Recent cyberattacks require us all to be vigilant." *Microsoft,* October 4, 2019. https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/

[154] DEF CON. https://www.defcon.org/

[155] Peter Hirschfeld. "Ethical Hackers Breach Vermont Voting Machines, But Officials Say No Need to Panic." *VPR,* August 20, 2019. https://www.vpr.org/post/ethical-hackers-breach-vermont-voting-machines-officials-say-no-need-panic#stream/0

[156] Kim Zetter. "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials." *Vice.* August 8, 2019. https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

[157] Kim Zetter. "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials." *Vice.* August 8, 2019. https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

[158] "California Cybersecurity Integration Center." *California Office of Emergency Services.* https://www.caloes.ca.gov/cal-oes-divisions/law-enforcement/california-cybersecurity-integration-center

[159] Staff Report from Georgia CEO. "Governor: Budget Priorities Cybersecurity, Education, Public Safety." *Middle Georgia CEO,* January 12, 2017 http://middlegeorgiaceo.com/news/2017/01/governor-budget-prioritizes-cybersecurity-education-public-safety/

[160] Theo Douglas. "Cybersecurity, IT Centralization Are Focuses for Santa Clara County CIO." *Government Technology,* January 3, 2018. https://www.govtech.com/dc/Cybersecurity-IT-Centralization-Are-Focuses-for-Santa-Clara-County-CIO.html

[161] Andy Chow. "Ohio Working With Local Governments To Enhance Cybersecurity." *Statehouse News Bureau,* July 5, 2019. https://www.statenews.org/post/ohio-working-local-governments-enhance-cybersecurity

[162] Maggie Miller. "Senators introduce bill to strengthen cybersecurity of local governments." *The Hill.* October 30, 2019. https://thehill.com/policy/cybersecurity/468210-senators-introduce-bill-to-strengthen-cybersecurity-of-local-governments

[163] Eduard Kovacs. "Senate Passes DHS Cyber Hunt and Incident Response Teams Act." *SecurityWeek,* October 1, 2019. https://www.securityweek.com/senate-passes-dhs-cyber-hunt-and-incident-response-teams-act

[164] LA Cyber Lab. https://www.lacyberlab.org/

[165] Sean Gallagher. "Los Angeles partnership launches platform to help people catch phishes." *Ars Technica*, September 18, 2019. https://arstechnica.com/information-technology/2019/09/los-angeles-partnership-launches-platform-to-help-people-catch-phishes/

[166] "IBM Cyber Range Experience for the Public Sector." *SecurityIntelligence,* December 11, 2019. http://ibm.biz/cyber-range-cities