DEPARTMENT OF PUBLIC SAFETY

NEVADA OFFICE OF CyberDefense COORDINATION

Annual Report 2018

Table of Contents

Executive Summary

The financial consequences of a cyberattack are growing substantially, according to a recent study conducted and developed by Ponemon Institute and Accenture. Information collected from hundreds of companies in seven countries, including the United States, revealed a 22.7% increase in the global average cost of cybercrime – now costing individual companies approximately $11.7 million per year. Unfortunately, prevailing belief among cybersecurity experts is that the cyber threat landscape will likely become worse, before improving. Massive data breaches of 2017, including: Equifax, Blue Cross Blue Shield / Anthem, Yahoo, and Verizon – to name a few – resulted in the loss of hundreds of millions of sensitive personal records, impacting nearly half of the U.S. population – the Equifax data breach alone impacted 1.2 million Nevadans.

"This past year, cyber criminals caused major service disruptions around the world, using their increasing technical proficiency to break through cyber defenses. In 2018, we expect the trend to become more pronounced as these attackers will use machine learning and artificial intelligence to launch even more potent attacks." – Symantec

While organizations increase efforts to bolster security, cyber actors continue to not only increase the volume of attacks each year, but also develop new and diverse attack methods, as well as mechanisms to cover their tracks. Additionally, recent government leaks have fueled access to advanced exploitation tools. Less sophisticated hackers will continue to leverage these tools to achieve their financial, ideological, or political goals.

Further, a greater and increasingly detrimental component of cybersecurity, which is often overlooked, is the human cultural aspect of cybersecurity. Rapid advancements in technology and day-to-day reliance of computing and networked devices over the last several decades have created untold improvements to society – but at a cost. The human connection to a cyber threat is hampered do to the abstract nature of the cyber landscape. This abstraction creates a significant gap between what the average individual perceives as the consequence of a cyber threat and the actual consequence they may endure following a cyberattack. Humans are hardwired to understand the consequences of physical threats and violence, while comprehension of a non-physical threat or attack is still in development. Malicious cyber actors will continue to exploit this social vulnerability with great success until the human culture disconnect is eliminated.

Despite the number of challenges ahead, the Nevada Office of Cyber Defense Coordination is spearheading efforts to address the cyber threat across the State. Although only in existence for a short period, OCDC has developed an extensive array of partnerships throughout the State, which continues to prove successful in galvanizing cybersecurity stakeholders. Partnerships developed between federal entities and states with long-standing cyber programs have facilitated the exchange of valuable information and best practices, advancing OCDC capabilities more efficiently. Further, working in close partnership with the University of Nevada – Reno, OCDC aided in the creation of a no-cost cybersecurity tool, which will enable partnering entities to enhance protection of their information technology infrastructure. Moving forward, OCDC will leverage and bolster the wide-ranging network of cybersecurity partners within the state to meet the strategic goals of the Office. Collaboration, education, and action will be key factors to combat the advancing cyber threat. However, OCDC is well positioned to champion tangible change in the cyber threat landscape, ultimately improving Nevada communities.

Overview

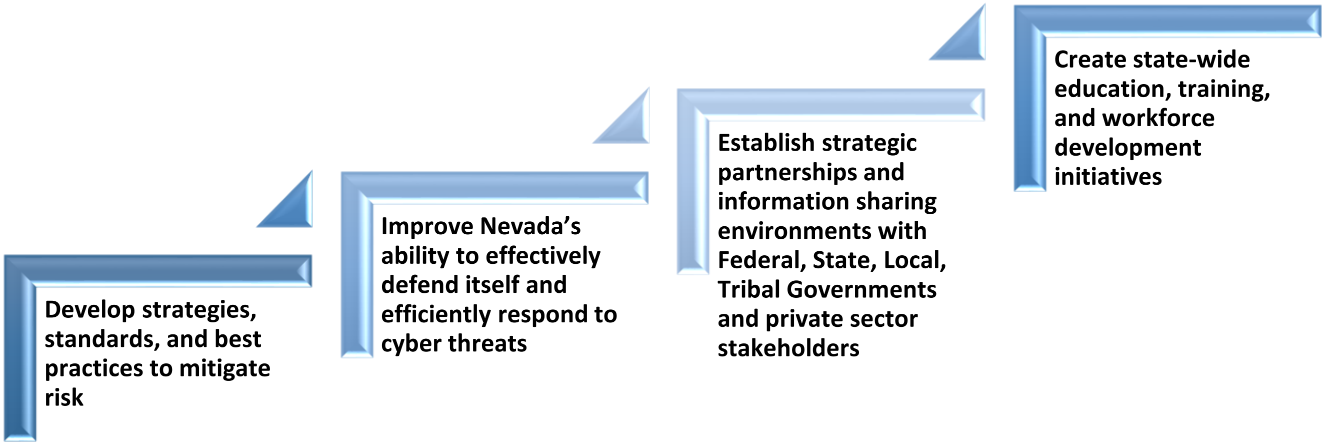
The inception of the Nevada Office of Cyber Defense Coordination (OCDC) stems from Nevada Governor Brian Sandoval's vision and initiative to champion cybersecurity across the State of Nevada. Announced as a leading priority during the Governor's 2017 State of the State address, OCDC gained traction as Assembly Bill 471 and received a wealth of support from myriad government and non-government organizations across the state. On June 2, 2017, Assembly Bill 471 was passed into law, establishing the Nevada Office of Cyber Defense Coordination. OCDC is housed under the Nevada Department of Public Safety, allowing for simplified coordination of support resources.

The Office of Cyber Defense Coordination engages with state and partner components for the synchronization and coordination of strategic cybersecurity initiatives within Nevada. The Office of Cyber Defense Coordination does not replicate existing programmatic or budgetary mechanisms, or interfere with previously defined cybersecurity roles; rather, it provides a single platform to integrate cybersecurity initiatives, manage strategic policy and planning, and streamline cybersecurity governance structures. Further, OCDC provides senior-level advice and recommendations on key cyber issues to the Governor's Office, Nevada State Legislature, state agencies, political subdivisions, tribal governments, private-sector entities, and the Nevada Commission on Homeland Security.

Mission and Vision

OCDC Mission: The Nevada Office of Cyber Defense Coordination serves as the primary focal point for cybersecurity strategy, policy, planning, and coordination for the State of Nevada.

OCDC Vision: To become a State leader in cybersecurity information management, by coordinating information, enabling effective risk-management decisions, addressing cyber threats and advancing cybersecurity education and training. Key objectives include:



Develop strategies, standards, and best practices to mitigate risk

Improve Nevada's ability to effectively defend itself and efficiently respond to cyber threats

Establish strategic partnerships and information sharing environments with Federal, State, Local, Tribal Governments and private sector stakeholders

Create state-wide education, training, and workforce development initiatives

Organizational Activities

This section of the report outlines the progress made by the Nevada Office of Cyber Defense Coordination from October 1st, 2017 to June 30th, 2018. Funding authority for Nevada Office of Cyber Defense Coordination staff did not take effect until October 1, 2017, limiting the operational window of the Office.

Staff

On October 23, 2017, the Office Administrator was appointed. Recruiting for, and hiring of additional Office staff consumed several months following funding authority, as the unique duties and role of the Office proved difficult to match against potential candidates. However, the Office reached full staffing on June 4th, 2018.

Strategic Plan

To address the increasingly diverse cyber threat environment, the Nevada Office of Cyber Defense Coordination implemented a comprehensive cyber strategy to deter state and non-state actors from conducting malicious cyber activity against the State of Nevada and its interests. The Nevada Office of Cyber Defense Coordination is currently developing a framework to enable the State of Nevada to work with public and private stakeholders to effectively respond to and mitigate the impact of cyberattacks in Nevada.

The specific goals outlined in the OCDC strategic plan represent the first step to realizing an improved cybersecurity posture across the State of Nevada. The strategies contained within identify essential and achievable goals to enable and empower entities across the State of Nevada to improve their unique cybersecurity posture. Further, these strategies contain goals for improving cybersecurity education, training, and bolstering the cybersecurity workforce in Nevada. Primary OCDC strategies are as follows:

- Strategic Goal 1: Adopt Information Management Policies, Guidance, and Best Practices
- Strategic Goal 2: Safeguard Information Systems against Cyber Threats
- Strategic Goal 3: Develop Incident Response, Triage, and Recovery Teams
- Strategic Goal 4: Foster Partnerships to Strengthen Cyber Ecosystem
- Strategic Goal 5: Champion Cyberecurity Education and Training

To view the Nevada Office of Cyber Defense Coordination Strategic Plan in its entirety, please use this link: http://dps.nv.gov/uploadedFiles/dpsnvgov/content/divisions/OCDC/home/Nevada-Office-of-Cyber-Defense-Coordination_Strategic-Plan_2018%202020.pdf

Protection of State Information Systems

To address the protection and security of state information systems essential to protecting the health, safety, and welfare of the people of Nevada, the Nevada Office of Cyber Defense Coordination initiated a collaborative partnership with the Nevada Department of Administration – Office of Information Security (OIS). OIS is comprised of information security specialists who provide professional services to support the development and administration of State enterprise and independent agencies' information security programs across Nevada government. While efforts are only initial at this time, OCDC and OIS – as well as the State of Nevada Office of the State Chief Information Officer (CIO) – are currently developing a charter to delineate activities and future goals.

Partnership development with the State CIO stalled for a period of months, as the position was vacant. Following the hiring of the CIO, efforts to build collaborative relationships and effectively move State cybersecurity efforts forward have proven very productive. The State CIO, as well as the Office of Information Security – managed by the State of Nevada Chief Information Security Officer – have focused efforts on bolstering State cybersecurity by improving enterprise-wide security maturity.

While recent improvements have proven effective for addressing cyber-related incidents, a number of long-term issues continue to linger, which prohibit holistic cybersecurity evolution at the state-level. Key decision-makers in the state have a wealth of opportunity to execute necessary change to advance cybersecurity. A sea-change within state government will prove critical in reducing cyber risk and improving the State's cybersecurity posture.

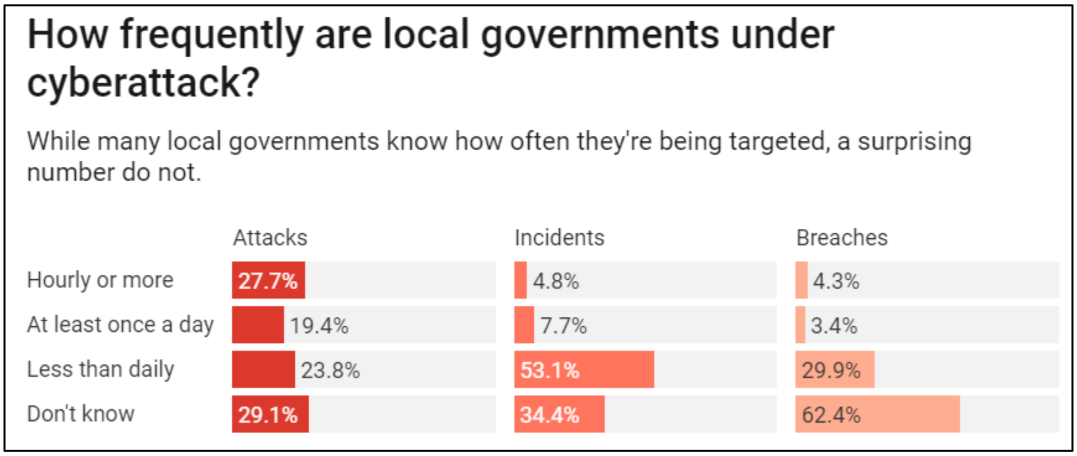
> *"By 2020, 100% of large enterprises will be asked to report to their boards of directors on cybersecurity and technology risk at least annually, which is up from today's 40%." - Gartner*

Additional challenges to reducing cyber risk lie in the relationship between those tasked with the responsibility of cybersecurity and key decision-makers within the State. Historically, Information Security – as well as other entities within the Executive Branch – are responsible for developing strategies and an associated budget to meet their legislative requirements. For many organizations, this process works perfectly to execute their mission. However, as the cyber threat increases in size and complexity, department heads, executives, and key decision-makers need to take a more active role in cybersecurity risk-management.

Under the current model, cybersecurity staff are responsible for determining and prioritizing cyber risk to the State, with limited interaction with key decision-makers. This has been the standard methodology for information security execution in business for decades. However, industry leaders are now shifting towards a more hands-on approach to cybersecurity. This enables key decision-makers to be more knowledgeable about cybersecurity from a strategic perspective and allows for their own determinations and priorities as it relates to cyber risk to the business. Through increased interaction between key decision-makers and OCDC/OIS, the State of Nevada would see immediate dividends, and set the bar for surrounding states when it comes to the successful implementation of information security initiatives.

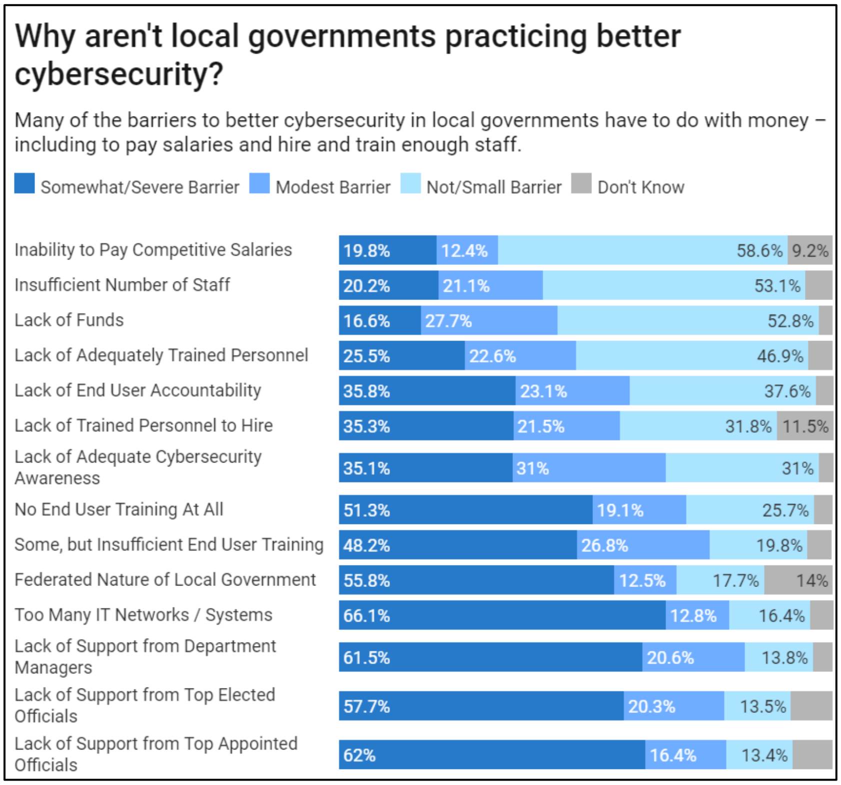
An additional area to aid in the protection of State information systems and the delivery of essential services to residents and visitors of Nevada focuses on increased resource allocation to the Executive Branch for cybersecurity. When compared to other states in the U.S., Nevada falls short. A number of states spend approximately 5% of annual Information Technology spending on cybersecurity, while Nevada has consistently earmarked approximately 2% of Information Technology budget on cybersecurity.

In 2016, the University of Maryland, working in partnership with the International City/County Management Association, conducted the first-ever nationwide survey of local government cybersecurity. According to their research, approximately 44% of survey respondents indicated they experienced cyberattacks on a daily basis.



Attacks are attempts to gain unauthorized access to cause mischief or do harm. Incidents are events that compromise confidentiality, integrity or availability of a computer system. Breaches are incidents that result in confirmed disclosure of information to an unauthorized person. Source: University of Maryland, Baltimore County.

Despite the significant volume of sensitive personal, health, criminal, etc., records local governments house and manage, most local governments are either unaware or unsupportive of cybersecurity, as indicated by the chart below:



Outreach

Efforts to develop an effective statewide cybersecurity strategy requires an extensive understanding of the unique and important organizational and individual needs throughout Nevada. For these reasons, the OCDC Administrator held meetings with over 70 different organizations across the state in this reporting period. Organizations ranged from federal, state and local government entities, to academia and private-sector entities. Gaining insight to the successes and challenges of these entities is critical for the development of a state strategy. Further, outreach efforts created opportunities to offer additional insight into available resources, current trends, and information.

Outreach activities were additionally successful in identifying gaps in cybersecurity experienced by rural partner communities, which constitutes an important component of the State. A number of rural organizations in Nevada have little or no staff directly assigned to cybersecurity. Often, the role of cybersecurity is tasked as an additional duty, or provided through a third-party vendor. OCDC staff met with CIO and/or IT Directors/Managers in over half of Nevada's counties (some counties contract out their entire IT department – other counties have unfilled positions). Cybersecurity maturity levels varied significantly county-to-county, but most experience similar challenges – lack of funding, authority, and professional development training. As indicated in the previous section, the importance of cybersecurity struggles to resonate with appointed and elected officials. This dynamic likely proves increasingly detrimental in rural and frontier counties, not unlike those across the State of Nevada.

OCDC is dedicated to supporting disparate and geographically challenged entities across the State of Nevada. Rural and frontier entities are often limited in resources, particularly concerning cybersecurity. For these reasons, OCDC will continue to champion the needs of these entities and help support access to a variety of resources, tools, information, and training.

Education and Workforce Development Projects

In Nevada, there are currently multiple programs focused on building a robust cybersecurity workforce. At all levels of education, Nevada is beginning to grow its cybersecurity education capabilities to facilitate this workforce development.

In April of 2018, the Department of Homeland Security (DHS) and the National Security Agency (NSA) recognized the College of Southern Nevada (CSN) as a National Center of Academic Excellence in Cyber Defense (CAE-CD). The CAE-CD program provides additional funding to its designees, which allow CSN to share curriculum and resources with other schools in an effort to bring them up to the same standard. So far, CSN has started working with Great Basin College in Elko and Truckee Meadows Community College in Reno.

> *"In the ongoing battle to secure organizations from malicious actors that commit crimes through methods such as theft, destruction or data manipulation, frontline defenders are a scarce resource. As the demand for skilled personnel capable of meeting the challenges posed by these threat actors continues to rise, the supply simply cannot keep pace." – FireEye M-Trends Report 2018*

Recently CSN cyber educators were part of a Nevada team that wrote the standards for Nevada high school members to earn career, and technical (CTN) education credits in cybersecurity. [i] The credits count as college credits. Prior to CTE credit approval, Nevada educators at Cheyenne High School in Las Vegas wrote their own cybersecurity courseware as an interim fix – speaking to the passion educators have about cybersecurity in the State of Nevada. Additionally, Cheyenne High School hosted a Girls Go CyberStart competition and the high school had the highest number of registrants — 290 — in the entire nation. The game provided young women the chance to discover their talents in cybersecurity and learn about careers in the field.

The University of Nevada, Reno (UNR) – though not currently designated as a CAE-CD – continues to excel in cybersecurity training and education. In 2014, UNR established the UNR Cyber Security Center, which supports economic development in Nevada through education, research, and outreach to industry, by addressing the growing national challenge of cybersecurity. In 2018, the UNR Cyber Club participated in the National Cyber League competition and three of the members finished in the top 10% of over 3k competitors.

The Desert Research Institute (DRI) is hosting a DRI Cybersecurity Internship Program in partnership with the SANS Institute. The internship, which will run from August through December 2018, is open to residents of Nevada, including high school graduates, college students, and/or individuals interested in a career change. Applicants compete to earn one of several positions in the program, which includes a scholarship for the SANS CyberStart Essentials course, the CyberStart Essentials certification exam, and a 120-hour hands-on cybersecurity internship at DRI.

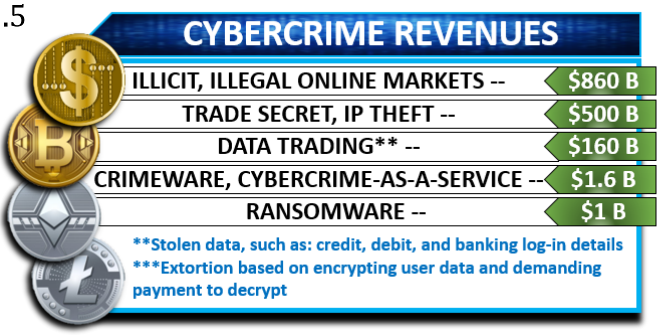
In January 2018, the president of the Southern Nevada Cybersecurity Alliance (SNCA) and the Chancellor of the online Western Governors University (WGU) launched two cybersecurity scholarships. Both organizations are committed to providing corporate funded educational opportunities for those seeking to advance in the field of cybersecurity.

Cybersecurity Education is key to the United States and Nevada's cyber defense. Cybercrime continues to eclipse cybersecurity professionals trained to defend against it by a margin of 3 to 1. In 2017, the U.S. employed nearly 780k cybersecurity professionals, yet still had 350k cybersecurity job openings.[ii] At the current rate, the U.S. is on pace to hit a half-million or more unfilled cybersecurity positions by 2021. Nevada currently has an estimated 1700 cybersecurity jobs unfilled.[iii] While some organizations are making efforts to meet this demand, a cybersecurity education cultural shift must be embraced, from the newest IT professional working in critical infrastructure, to Congress. Every moment, of every day, the world grows more interconnected through technology. By 2022, there will likely be 6 billion internet users, which is approximately 75% of the entire world population. The same math predicts that by 2030, the number of internet-connected users will reach 90% of the world's projected 8.5 billion people. The State of Nevada cannot afford to wait for neighboring states and countries to train cybersecurity professionals. Nevada must educate the next generation of cybersecurity professionals now to protect and grow its cyber future.

Cyber Threat Overview

The financial consequence of a cyberattack is getting worse, according to a recent study conducted and developed by Ponemon Institute and Accenture. Information collected from hundreds of companies in seven countries, including the U.S., revealed a 22.7% increase in the global average cost of cybercrime – now totaling individual companies approximately $11.7 million per year. In February 2018, the United States Executive Office of the President - Council of Economic Advisers reported an estimated economic loss between $57 billion and $109 billion in 2016, due to malicious cyber activity.

In 2017, global cybercrime accounted for an estimated $1.5 trillion in revenues and is expected to exceed that amount in 2018[ivv]. Small business, the medical and healthcare industry, government/military, and educational institutions were the primary targets of cyberattack in the United States. In the first half of 2018, cryptojacking – the unauthorized use of someone else's computing resources to mine cryptocurrency – has outpaced ransomware as the number one threat for businesses and individuals[vi].



CYBERCRIME REVENUES	
ILLICIT, ILLEGAL ONLINE MARKETS --	$860 B
TRADE SECRET, IP THEFT --	$500 B
DATA TRADING** --	$160 B
CRIMEWARE, CYBERCRIME-AS-A-SERVICE --	$1.6 B
RANSOMWARE --	$1 B

**Stolen data, such as: credit, debit, and banking log-in details
***Extortion based on encrypting user data and demanding payment to decrypt

Ransomware

Ransomware infections spiked in 2016, earning the nickname, “The year of ransomware.” In 2015, cybersecurity experts discovered 29 different ransomware strains, this number shot to 247 in 2016, representing an astounding 752 percent increase. Ransomware attackers generated significant profits raking in a reported $1 billion. Much of this was the result of attacking large businesses without data backups, making ransom demands more successful for cybercriminals.[vii]

In 2017, effective ransomware attacks continued, including large-scale infections like WannaCry and NotPetya, which impact businesses, government organizations and utility providers across the globe. In addition, The Verge reported in late June 2017 that another new ransomware – initially thought to be a variant of Petya – was impacting users leveraging the same EternalBlue exploit utilized in WannaCry infections. The newer strain is called “NotPetya.” [viii]

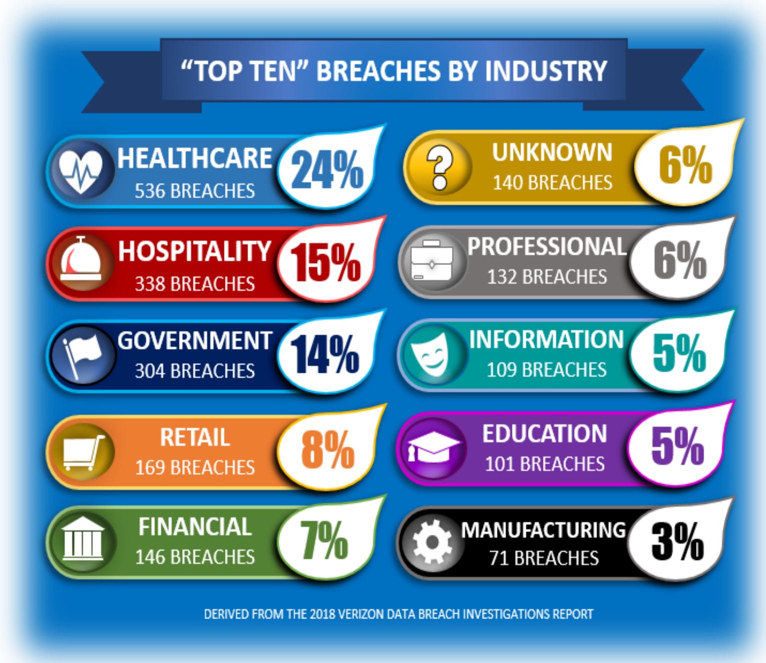
WannaCry malware was used to execute a ransomware attack in more than 150 countries, locking down over 300,000 computers in industries ranging from health care to car companies. WannaCry financial damages ranged from hundreds of millions to billions of dollars[ix]. Security experts believe North Korea was behind the attacks.

Additionally, in June of 2017, the NotPetya ransomware cyberattack was launched in Ukraine, eventually spreading throughout Europe, India, and the United States. NotPetya, based on a prior identified ransomware known as Petya, is designed without the ability to decrypt files it had already encrypted, therefore effectively destroying the data. NotPetya’s impact included Ukraine’s Chernobyl Nuclear Power plant, a U.S. pharmaceutical company, multiple U.S. hospitals, and shut down India’s largest shipping port. The attack – considered the most destructive cyberattack to date – infected tens of thousands of systems in more than 65 countries, with a financial impact in the billions. [x,xi] Security experts believe the Russian military was behind the attack and Ukraine was the primary target; the Government of Russia vehemently denies this claim.

Data Breaches

According to the 11th Annual Verizon Data Breach Investigations Report (DBIR), there were 2,216 confirmed data breaches worldwide between November 1, 2016 and October 31, 2017. Data breach statistics represent *confirmed* disclosure – not potential exposure - of data to an unauthorized party.[xii] Often, due to legal requirements, not all breaches are reported or disclosed to the public. Overall, the majority of breaches were perpetrated for financial gain followed by strategic advantage, often referred to as espionage. Almost 90% of all breaches fall into these two categories. Additionally, despite botnet activity, Phishing (social engineering), installation of key loggers (Malware), and use of a backdoor or use of stolen credentials (Hacking), represent the most common breach methodologies.

In 2018 there have been multiple data breach events involving Nevada citizens and their information. In April 2018, Dignity Health, a major health system that operates 39 hospitals and 400 care centers in California, Nevada, and Arizona, suffered a data breach of 56k patient records. The breach was not reported until May 31, 2018. Additionally, Dignity hospitals in Nevada reported a breach of 6k patient records, this breach occurred in mid May 2018. In December 2017, a Texas-based restaurant chain notified 2 million customers in 15 states – including Nevada – that a RAM-scraping malware was used to infiltrate payment processing systems. This is the same malware used during the Target Store data breach in 2013, which impacted up to 40 million customers. In December 2016, a data breach on Nevada’s medical marijuana program database exposed the personal information of approximately 11.7k Nevada residents.



Although large-scale breaches of high profile companies has become the norm, the federal government has also been marred by data breaches. According to a 2017 Government accountability Office (GAO) report, the U.S. federal government has multiple shortcomings when it comes to the protection of federal information systems.[xiii] Breaches addressed in the GAO report included the Internal Revenue Service, Federal Election Commission, Department of Labor, Securities and Exchange Commission, Federal Deposit Insurance Corporation, Department of State, Energy, Homeland Security, and Defense, the U.S. Postal Service, and multiple U.S. Military entities.

Aside from the continued barrage of attacks aimed at federal entities, the public sector continues to face its own challenges. The DBIR highlights that public administration accounts for almost 23k cyber incidents, which resulted in 304 confirmed data breaches. Local governments took the brunt of "social-attacks" which account for 93% of all security incidents. The public sector was the top industry targeted by social engineering breaches, with 92 breaches, and healthcare registering 62 breaches. Overall, despite the widespread use of ransomware, the simple phishing email was the number one tactic used in public sector breaches. Cyberespionage, defined to include "unauthorized network or system access linked to state-affiliated actors" and/or with an espionage motive, was the top recognized pattern for the public sector, identified as being behind 10,311 incidents and 77 breaches. Often times, espionage cases begin with phishing, which then lead to pretexting — and move from email to telephone and even personal dialogue.

In the 2013 DBIR, ransomware was first mentioned as having the potential to be the "tool of choice" for cyber criminals; that statement has proven true. Ransomware has overtaken all other types of malware to be the most prevalent variety of malicious code for the DBIR reporting period. Ransomware evolved from only encrypting a single computer to now being capable of infecting, encrypting, and damaging or even destroying entire file servers and databases, all from a single point of entry. Although ransomware is the tool of choice, of 444 million malware detections across approximately 130,000 organizations, the majority of companies only received malware on six or fewer days a year.

The most notable breaches in 2017 were ranked by the Breach Level Index.[xiv] The ranking system allows for breaches to be categorized numerically from minimal risk to catastrophic risk. The following represent catastrophic data breaches in 2017.[xv]

- **Equifax**: Malicious actors infiltrated Equifax's systems by exploiting a weak point in the credit bureau's website software. 147.7 million U.S. consumers were affected.
- **Deep Root Analytics**: A data firm contracted by the Republican National Committee, Deep Root Analytics, stored personal information on nearly all 200 million American voters for two weeks on Amazon's cloud storage service without proper password protections.

- **Kennesaw State University**: The University contacted the FBI regarding a breach at its Center for Election Systems. The event possibly compromised as many as 7.5 million voter records.
- **Alteryx**: An Amazon Web Services storage bucket was left open to the public by marketing analytics firm Alteryx. The breach exposed the sensitive information of more than 120 million American households, including the names of residents, income, mortgage rates, and even residents' interests/hobbies.
- **River City Media**: The email marketing organization failed to properly configure backups, thereby making its data publicly viewable online. The breach exposed 1.34 billion email addresses, used for spam in the form of "offers." The data also included customer names, physical addresses, and thousands of email addresses used by the company to circumvent anti-spam filters.

Data analyzed since 2016 indicates security incidents are considerably more frequent and larger in scope. The number of records breached nearly doubled in the span of a year.[xvi] Breaches shared many commonalities that indicate how cybercriminals were so successful in their breach attacks. A lack of proper safeguards and training in the form of accidental data loss produced billions of data breaches. Relatively few data breaches occurred where encryption was utilized, overall, data breaches involving encrypted data fell 33.7%. Malicious outsiders compromised hundreds of millions of records and accounted for 73% of all data breach incidents worldwide. These three common findings indicate a need for cybersecurity policies to address a standard of encrypting all sensitive data, storing and managing all encryption keys, and controlling access and authentication of all users who access the data. In today's day and age, any security strategy must be built around the understanding that the secure movement and sharing of data is fundamental to the success of an organization.

Hacking Tools

In mid-2016, a hacker group by the name of The Shadow Brokers released several hacking tools attributed to the National Security Agency (NSA). The tools focused on exploiting enterprise firewalls, antivirus software, and Microsoft products.

In March 2017, Wikileaks published an extensive collection of stolen government documents referred to as "Vault 7." The files contain an array of Central Intelligence Agency (CIA) hacking tools, including: malware, viruses, trojans, weaponized 'zero day' exploits, malware remote control systems and associated documentation.[xvii] Wikileaks allegedly obtained the classified hacking tools from a (former) CIA engineer, who was indicted on a host of Espionage Act violations in June 2018. Security experts indicate the release of classified hacking tools significantly impact intelligence community operations. Additionally, the release of these tool essentially provided anyone access to nation-state-level hacking tools.

Within days of the Shadow Brokers release, cyber criminals started using EternalBlue to extract passwords from browsers, and to install malicious cryptocurrency miners on target devices. Even a year after Microsoft issued a patch, attackers still rely on the EternalBlue exploit to target victims, because so many machines remain defenseless to this day. In February 2018, cyber criminals used EternalBlue to install cryptocurrency-mining software on victim computers and servers. The exploit is ideal for many attackers because it leaves very few digital traces. In March 2018, Symantec published findings that Iranian hackers used EternalBlue to attack targets around the Middle East, focusing on transportation groups like airlines, aircraft services, industry technology firms, and telecoms. It will likely be years before enough computers are patched against EternalBlue that hackers retire the exploit from their arsenal.

Critical Infrastructure

Following the hack of the Democratic National Committee in 2015, as well as Russian influence of the 2016 presidential election, DHS determined the election infrastructure required additional protections. In early 2017, election infrastructure was designated as part of the nation's critical infrastructure as a subsector under the Government Facilities sector. Under the designation, Department of Homeland Security (DHS) – through its National Protection and Programs Directorate (NPPD) – provides an array of services that state and local election officials can utilize to reduce both cyber and physical risk to their election systems and facilities. The designation allows DHS to provide services on a prioritized basis at the request of state and local election officials. The designation also brings the structure and support of the National Infrastructure Protection Plan (NIPP) to bear on behalf of the election infrastructure community. NIPP advances critical infrastructure security and resilience through partnership and innovation.[xviii]

Legacy Systems

In addition to the advent of new technologies, and the subsequent cybersecurity risks associated with any technological advance; the prevalence of legacy software and hardware systems in the U.S. and abroad presents a wealth of cybersecurity concerns. It is estimated that almost 4% (or 16.5 million devices) of all devices in the U.S. run software that is no longer patched by vendors; generally web browsers, java applications, and operating systems are among the top offenders.[xix] Security experts believe that percentage is considerably higher in the business and industrial arena. This is likely due to restrictive policies, legal barriers, warranty, and certification concerns, not to mention associated costs. The cost of upgrading legacy systems can be astronomical. An average small business will have approximately 800 employees who all use a separate computer or device that must be kept up to date. A larger business may have tens of thousands of computers to keep updated. On top of all this, legacy systems and software pose concerns for redundancy, scalability, and increased failure rates.[xx]Lastly, legacy systems often hinder the sharing of information between systems on the same network; this creates data silos that can't be accessed easily and can't be backed up effectively.

Cyber Threat Summary

The cyber threat is not going away. It is clear that the amount of internet-connected users is going to continue to grow and thus the number of cybercriminals will continue to grow. Every aspect of cyber culture, private, public, and education will continue to be vulnerable and must adapt to the changing landscape of cybersecurity. Today, most critical systems are interconnected and driven by a computer of some type. Personal lives will be reliant on virtual assistants, and IoT will be part of practically every facet of daily life for all people. While cryptojacking may pose the most prevalent threat to security at this time, the future holds even greater obstacles to cybersecurity. Medical devices, installed in humans, are susceptible to cybercriminals, biometric data, such as fingerprints, face recognition, DNA, palm prints, iris recognition, etc., currently used to secure many parts of our daily lives, will become a commodity for cybercriminals.

As the number of internet-connected users grows, Nevada must position itself to cope with and protect enormous amounts of user data. Nevada will need to develop and support mechanisms for training and developing the next generation of cyber experts who know how to create and drive advanced cyber defense systems and policies. Now is the time for Nevada to look to form new cyber professions and expertise in those professions through education and training initiatives. Nevada must develop policies that ensure it is prepared to take a leading role in the protection of its infrastructure, such as power grids, water supplies, traffic controls, and quite possibly *everything* attached to the internet. [xxi]

Near-Future Goals and Objectives

> *"The impact of a breach goes beyond the cost of remediation. The costs of investigations, notifications, and putting controls in place to prevent future events is the tip of the iceberg. Post-breach lawsuits are on the rise, fines are being level, C-levels are being held accountable, and company values are often plummeting, costing millions more." – Foresite*

ESF-Cyber

The Nevada Office of Cyber Defense Coordination is currently working in partnership with the Nevada Division of Emergency Management, as well as additional stakeholders including the Department of Public Safety - Division of Investigation, the Nevada National Guard, and several county-level Emergency Managers, to develop an Emergency Support Function (ESF) for Cyber. Current efforts align with the National Incident Management System, which conforms to both Federal Emergency Management Agency (FEMA) and Department of Defense (DoD) standards. The new ESF for Cyber capability is projected to be online later this year.

Cyber Pipeline

Despite the number of positive education and training activities at play across the state, immense opportunity exists to formalize and scale the path from K-12 and college-level education and training, to a professional cybersecurity career in Nevada. While this process somewhat exists currently, it is isolated, and relies on a handful of dedicated individuals who are passionate about cybersecurity and improving the lives of young people throughout the community. Leveraging the lessons of these dedicated individuals, OCDC will develop a Cyber Pipeline to aid in the process of identifying individuals interested in cybersecurity, facilitate access to education, training, and certification for those individuals, facilitate follow-on internships for real-world experience, and finally, job opportunities. Understanding the extreme lack of qualified personnel to meet the cybersecurity labor demand, Nevada must invest in cultivating our own professional workforce.

Education

Regrettably, the term "cybersecurity" represents an array of different things depending on who you ask — there is no single definition in which most people immediately subscribe to regarding cybersecurity. This issue is problematic for a variety of reasons. Most notably, when discussing cybersecurity with the average (non-technical) person, they generally struggle to understand core aspects of cybersecurity and the impact of the cyber threat. This paradigm is increasingly problematic in the areas of business and government. Efforts to bridge this gap have fallen short. Through partnerships in academia and the private-sector, OCDC aims to develop mechanisms to better educate, define, quantify, and make cybersecurity tangible to the non-technical individual.

Cultural Shift

The education goal identified above represents a component of a larger-scale issue related to cybersecurity. Recent years have brought volumes of high profile incidents in major private-sector industries as well as government, shedding light on the global problem of the cyber threat. While these attacks have proven detrimental, they have also increased awareness of the cyber threat significantly. OCDC aims to continue educating the community on the societal impact of the cyber threat. Increased knowledge and cyber safety will decrease the effectiveness of a cyberattack, reducing community impact.

Conclusion

The cyber threat landscape continues to shift, and with few mature cybersecurity programs in existence – whether government or private-sector – the need for organizations to increase investments in agile and resilient security is paramount. Future efforts to combat the growing cyber threat will require extensive collaboration between stakeholders. The public, business decision-makers, and government officials can no longer afford to discount the cyber threat to their organizations and to society.

Despite an unwelcoming outlook for the near-future, a wealth of important and beneficial initiatives are currently in-work throughout Nevada. Individuals, businesses, government, and academia are challenging the status quo in cybersecurity. Diverse industries are bringing their unique talents and resources to bear, addressing the cybersecurity problem with the resources they can individually muster. Every level of academia has begun implementing programs that will train the next generation cybersecurity professionals.

The Nevada Office of Cyber Defense Coordination will continue to galvanize disparate groups to create a unified framework to counter the devastating effects of cyberattacks, increase access to information and best practices, cultivate a skilled workforce, and safeguard Nevada communities.

Sources

[i] https://www.csn.edu/cte

[ii] https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

[iii] https://www.cyberseek.org/heatmap.html

[iv] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[v] https://venturebeat.com/2018/04/21/the-web-of-profit-a-look-at-the-cybercrime-economy/

[vi] https://www.itproportal.com/features/bigger-than-ransomware-cryptojacking-is-the-new-money-maker/

[vii] https://blog.trendmicro.com/forecasting-the-future-of-ransomware/

[viii] https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

[ix] https://www.securityweek.com/impact-wannacry-ransomware-conversation

[x] https://www.securityweek.com/notpetya-attack-costs-big-companies-millions

[xi] https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/

[xii] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

[xiii] https://www.gao.gov/assets/690/682756.pdf

[xiv] https://breachlevelindex.com/

[xv] https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf

[xvi] https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf

[xvii] https://www.wired.com/2017/03/wikileaks-cia-hacks-dump/

[xviii] https://www.dhs.gov/topic/election-security

[xix] https://www.csoonline.com/article/2139382/data-protection/forgotten-risks-hide-in-legacy-systems.html

[xx] https://www.alvareztg.com/the-risks-of-outdated-technology-why-legacy-systems-cost-you-more-than-you-realize/

[xxi] https://cbi-blog.s3.amazonaws.com/blog/wp-content/uploads/2017/06/Cyber-Ai-Market-Map-6.17-body-image-3.png