Nevada Department of
Public Safety
Office of Cyber Defense Coordination

2018/2019

Annual Report

Table of Contents

Executive Summary

Cybersecurity is not getting easier. Whether public or private sector entity, the impact of digital crime is growing exponentially. The organizational cost of a cyberattack spiked more than $1.5 million in the past year; accelerating from $3 million per incident in 2018 to $4.6 million in 2019.[i] With that growth, organizations and individuals must be proactive in their cybersecurity planning, training, and reporting, or understand the potential risk consequences.

"Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades. Cyberattacks are the fastest growing crime globally, and they are increasing in size, sophistication and cost." – Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac

While organizations increase efforts to strengthen security, malicious cyber actors continue to not only increase the volume of attacks each year, but also develop new and diverse attack methods, resulting in significant financial losses, legal liabilities, and a reduction in business and community trust.

Cybersecurity Ventures predicts cybercrime will continue rising, and cost businesses more than $6 trillion annually, globally, by 2021. The estimate is based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation state sponsored and organized crime gang hacking activities, a cyberattack surface which will be an order of magnitude greater than it is today, and the cyber defenses expected to combat hackers and cybercriminals over that time.[ii]

Worldwide spending on information security products and services exceeded $114 billion in 2018, an increase of 12.4 percent from 2017, according to Gartner. For 2019, Gartner predicts the market to grow to $124 billion, and $170.4 billion in 2022.[iii] These figures underscore the significant impact of malicious cyber activity and serve as a bellwether for organizations not currently increasing investments in cybersecurity.

In spite of the number of challenges ahead, the Nevada Office of Cyber Defense Coordination (OCDC) is leading efforts to address the cyber threat across the State. OCDC continues to leverage an array of partnerships and collaborative relationships, which are vital to successfully 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. Communication, collaboration, education, and decisive action will be key factors to combat the advancing cyber threat.

Year in Review

During the course of the reporting year, the Nevada Office of Cyber Defense Coordination witnessed significant advancements in cybersecurity across the State of Nevada. Local government stakeholders converged to share ideas and best practices; educators advanced knowledge, training, and education opportunities; law enforcement organizations expanded their capabilities to address growing cybercrime; State Legislators passed valuable legislation to push cybersecurity forward in all corners of Nevada. These initiatives demonstrate some of the small pieces of the total effort made in the cybersecurity ecosystem in Nevada, many of which the Office of Cyber Defense Coordination supported, participated in, or helped facilitate.

Coordination

Over the last year, OCDC staff conducted over 75 organization-unique engagements with cybersecurity stakeholders in Nevada. Stakeholders ranged from federal, state, tribal, and local government agencies, to critical infrastructure, essential services providers, and private sector entities – the bulk of which continue to maintain close partnerships with OCDC.

Further, OCDC coordinated information and best practices, threat information, facilitated the building of relationships, access to resources, as well as participated in a number of local conferences, symposiums, and tabletop exercises. Despite the wealth of cybersecurity-related incidents shared and coordinated with OCDC, the OCDC Administrator did not convene an incident response team in this reporting period.

Items listed below represent a sampling of other notable activities:

Senate Bill 69

Throughout the 80th Legislative Session, OCDC worked in concert with the Nevada Department of Public Safety – Division of Emergency Management to spearhead Senate Bill 69(SB69). Joint efforts were realized in June 2019, when the Nevada Governor signed SB69 into law. The elements of SB69 mark a number of positive changes for both the Office of Cyber Defense Coordination, as well as cybersecurity as a whole in Nevada. The contents of the SB69 include:

- Designation of Cybersecurity Awareness Month in October of each year
- Nevada National Guard support to significant cybersecurity incidents (by request)
- Counties and incorporated Cities adopting and maintaining cyber incident response plans*
- Office of Cyber Defense Coordination quarterly reporting to the Governor
- Inclusion of private sector cyber incident information in public record request exemption
- Various administrative adjustments to core OCDC Nevada Revised Statute (NRS) mandates

* Over the course of the next several months, OCDC will develop and implement administrative rulemaking activities – in accordance with SB69, Section 9, 1 through 5 – to address cyber incident response of political subdivision (counties and incorporated cities).

More information is available here: https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6000/Overview

Election Security

Over the last several years, election security has proven a significant topic of interest and concern in the U.S. Malicious activity by nation-states, voting system infrastructure, funding, cohesive policy; all have an impact on safe and secure elections.[iv] For these reasons, OCDC provided support to the Nevada Office of the Secretary of State and the Clark County Election Department, leading up to the 2018 General Election. Over the next six months, OCDC staff will participate in an Election Security Policy Academy – sponsored by the National Governor's Association – to continue building improvements in election security. Nevada is one of six states selected in the U.S. for this academy.

Strategic Plan

In January 2018, 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 current strategies outlined below 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 Cybersecurity Education and Training

As the two-year strategic cycle approaches termination, OCDC will engage in an effort to create and publish a new and updated two-year statewide cybersecurity strategy.

Cyber Threat Overview

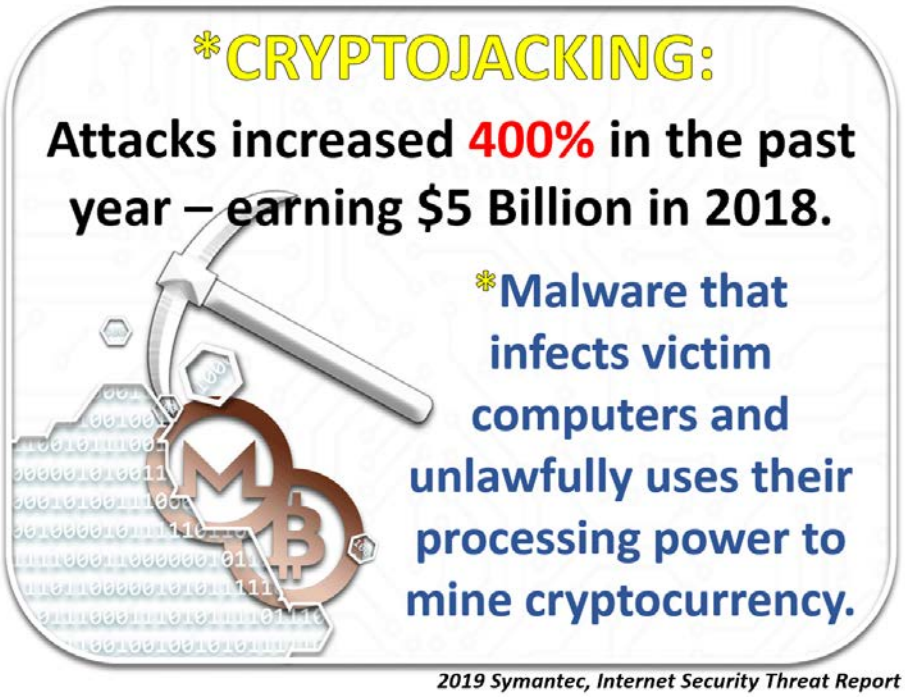
Necessity continues to be the mother of invention. As cybersecurity professionals continue their battle against cybercriminals in 2019, those same criminals continue to evolve their methodologies to outpace the efforts of cybersecurity professionals. The impact of cybercrime is also evolving. According to a recent study by Ponemon Institute and Accenture, the average cost of cybercrime per company now totals over $13 million per year, a 12-percentage increase over 2018, and a 72-percent increase over the past 5 years.[v]

Top 10 Most Valuable Information to Cyber Criminals.	Top 10 Biggest Cyber Threats to Organizations.
1. Customer Information - 17%	1. Phishing - 22%
2. Financial Information - 12%	2. Malware - 20%
3. Strategic Plans - 12%	3. Cyberattacks (to Disrupt) - 13%
4. Board Member Info - 11%	4. Cyberattacks (to steal money) - 12%
5. Customer Passwords - 11%	5. Fraud - 10%
6. R&D Information - 9%	6. Cyberattacks (to steal IP) - 8%
7. M&A Information - 8%	7. Spam - 6%
8. Intellectual Property - 6%	8. Internal Attacks - 5%
9. Non-Patented IP - 5%	9. Natural Disasters - 2%
10. Supplier Information - 5%	10. Espionage - 2%

EY – Global Information Security Survey 2018-2019

Further, the total annual cost of all types of cyberattacks is increasing. By 2021, cybercrime will cost the global economy over $6 trillion annually.[vi] Often, the cost of cybercrime includes damage that goes beyond the destruction of data and stolen money. These additional costs

include lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigations, restoration and deletion of hacked data and systems, and reputational harm. Many times, it takes years for an organization to recover from a cyberattack. Yet, according to estimates by Gartner, companies will increase cybersecurity spending by 9 percent in the coming year, which equates to only 2 percent of their total information technology expenditure.



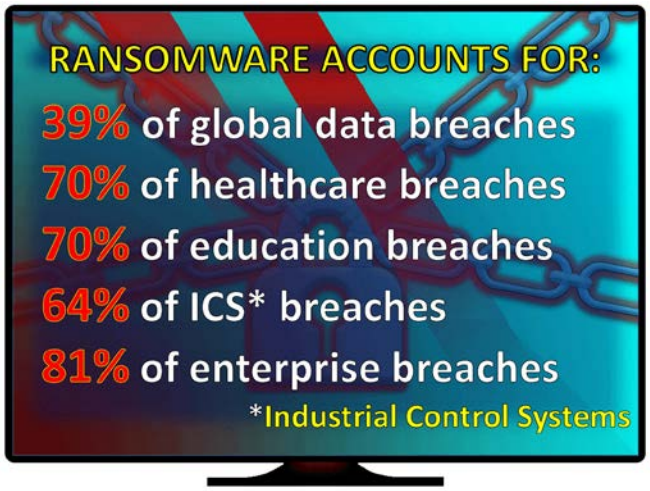
2019 Symantec, Internet Security Threat Report

The primary targets for cyberattacks mirror previous reporting with small business, healthcare, and financial institutions accounting for the majority of attacks in 2018-2019.[vii] Malware and web-based attacks continue to be the most expensive attack-type for U.S. companies, while ransomware and malicious insider attacks have grown the fastest over the last year.[viii]

Of note, the information security industry continues to struggle to define cybersecurity "attacks" and other related definitions. A common lexicon does not exist, which creates challenges quantifying malicious cyber activity. Attempting to find the "top cyberattack methods" for each industry, or political boundary, or even a country, is a daunting challenge – primarily due to research methodologies and data sets on cybersecurity attacks defined in different ways. An example of such a challenge would include, a phishing email can involve malware, so researches can choose to define them by either method.

Ransomware

For the first time since 2013, ransomware activity saw a drop of 20 percent in infections. In 2018, WannaCry, WannaCry clones, and Petya continued to inflate infection figures. When we remove the WannaCry/Petya data set from the statistics, the infection rate reflects a 52 percent drop for the year. [ix, x]



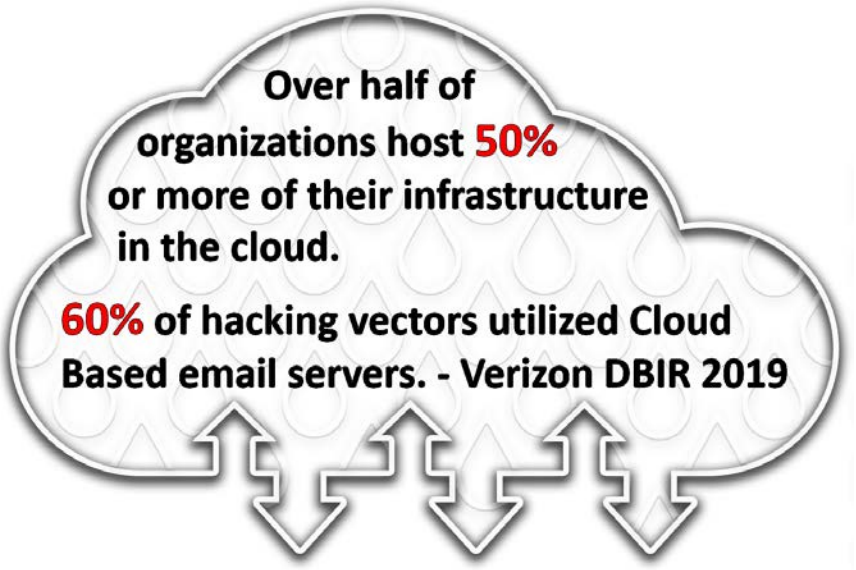
ENISA Threat Landscape Report 2018

Despite the lower number of infections in 2018, ransomware experienced a substantial evolution. Previously, consumers accounted for the majority of infections; however, recently the majority of reported ransomware infections have occurred in businesses. Enterprises accounted for 81 percent of all ransomware infections in 2018. This is likely due to business reliance on Windows-based computing and email as the primary communication tool for organizations - which most major ransomware families still primarily target. Additionally, a growing number of consumers are

exclusively using mobile devices, and their essential data is often backed up in the cloud, therefor much harder for ransomware to infect. [xi]

In addition to the evolution of targeting businesses, state and local government targeting* is on the rise.[xii] In 2016, State, Local, Tribal, and Territorial (SLTT) governments reported 46 ransomware attacks. In 2017, that number dropped to 38, which reflects a drop in ransomware attacks across all sectors during 2017. In 2018, that number jumped to 53, and in the first months of 2019, there have already been 24 reported attacks. At this time, only two states have no publicly reported ransomware attacks. ****Analyst Note**: SLTT attacks tend to be targets of opportunity; attackers appear to stumble into these targets. However, once a malicious attacker realizes they are in a SLTT target, they encrypt the most sensitive or valuable data.*[xiii]

Although ransomware attacks continue to decline in number, they remain a significant threat to security. In previous years, ransomware was utilized for indiscriminate attacks; however, in early 2019, a ransomware variant, *LockerGoga*, was used to target multiple manufacturing and chemical plants in Europe and U.S., which took weeks to remediate. LockerGoga execution required administrative rights that would have necessitated an attacker to have already gained some sort of privileged access to the network. Furthermore, while most ransomware tools use some level of obfuscation to avoid detection, there was very little of that in the LockerGoga use. This again suggests that the attacker had already analyzed the victim's network defenses and determined the malware would not be detected. Additionally, LockerGoga appears to lock victims out of their systems, thereby preventing them from even seeing or responding to a ransom note. This behavior seems indicative that physical destruction rather than ransom was the end goal. These trends exhibit a more tailored, targeted, and destructive approach to ransomware use.



An additional trending aspect of ransomware is whether the target should "pay or not pay?" Currently, SLTT governments are far less likely to pay a ransom than other sectors.[xiv] According to a 2019 CyberEdge report, 45 percent of organizations in non-SLTT sectors paid the ransom, where only 17 percent of SLTT entities confirmed ransom payment, while 70 percent confirmed they did not pay the ransom. Although SLTT governments may not pay ransoms nearly as often as other targets, they generate considerably more media coverage due to the effect of these attacks on the functioning of essential infrastructure and processes.

While OCDC is aware of a number of incidents involving ransomware over the reporting period, specifically in the private sector, OCDC did not receive any direct requests for support regarding ransomware in this reporting period. Further, OCDC received no information from government entities in Nevada indicating a ransomware event or a financial loss due to a ransomware attack.

Data Breaches

According to Statista and the 12th Annual Verizon Data Breach Investigations Report (DBIR), there were 1244 data breaches in 2018, (21 percent less than in 2017); those breaches exposed over 446.5 million records, a staggering 148 percent increase in volume from 2017.[xv] *Data breach statistics represent confirmed disclosure – not potential exposure - of data to an unauthorized party*.[xvi] 62 percent of breaches not involving an Error, Misuse, or Physical action (human error, misconfiguration, poor security practices, etc.) involved the use of stolen credentials, brute force, or phishing.

Cybercriminals utilized social engineering in 33 percent of data breach attacks, with phishing, pretexting, and bribery as the most common malicious actions. The most frequently compromised sets of data in breaches are internal information, credentials, personal data, medical information, and payment details.[xvii] Nation-state actors and their affiliates were involved in 23 percent of all breaches in 2018 and accounted for 79 percent of all breaches involving external actors. Additionally, 34 percent included internal actors, including former and collusive employees, who were part of a breach through misuse, which involved any unapproved or malicious use of organizational resources. [xviii]

As indicated in the 2019 DBIR, the time it takes for an attacker to move from the first action in the cyberattack chain to the initial compromise of an asset is short, typically measured in minutes. Conversely, 56 percent of 2018 breaches "took months or longer" to be discovered by the victim. This is why it is paramount for organizations to make biannual, or even quarterly, cyber threats assessments a standard, reoccurring event in order to highlight indicators of compromise and in turn rectify or mitigate identified issues before a loss of data occurs.

The following represent catastrophic data breaches in 2018-2019 worldwide.

- **Aadhaar**: The personal information of 1.5 billion citizens of India was exposed in a breach of the nations' ID database.[xix]
- **"Collection 1"**: 1.16 billion email addresses and passwords discovered by an IT security researcher and is thought to be the largest breach containing both unique e-mails and associated passwords to date.[xx]
- **Facebook**: 540 million users publicly exposed in two app datasets that were digitally stored in two Amazon Simple Storage Service (S3) storage buckets, according to a 2019 announcement by UpGuard.[xxi]
- **Marriott:** Exposed 500 million user accounts of Marriott's Starwood guest database.[xxii]
- **Exactis:** The personal information of 340 million U.S. consumers and business contacts exposed on a publicly accessible server.[xxiii]

Hacking Activities

As highlighted in the 2017/18 OCDC Annual Report, the trend of cybercriminals utilizing off-the-shelf hacking tools to conduct attacks remains steady. The "living-off-the-land" approach to being a cybercriminal shows no sign of diminishing. In 2018, multiple criminal groups continued to use Microsoft Office macros to propagate malicious payloads. Additionally, some cybercriminal groups do not use any malicious code; rather they relied exclusively on available tools to carry out malicious activity. Multiple cybersecurity agencies reported a massive 1,000 percent increase in PowerShell usage by cybercriminals. Symantec reported blocking on average 115k malicious PowerShell scripts each month, yet, this only accounts for less than 1 percent of overall PowerShell usage.

Supply chain attacks continued to be a feature of the threat landscape, with attacks increasing by 78 percent in 2018. Supply chain attacks, which exploit third-party services and software to compromise a final target, take many forms, including hijacking software updates and injecting malicious code into legitimate software. Also, a surge in *formjacking*—the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites—reinforced how the supply chain can be a weak point for online retailers and eCommerce sites.

Microsoft Security Intelligence Report Volume 24

Both supply chain and living-off-the-land attacks highlight the challenges facing organizations and individuals, with attacks increasingly arriving through trusted channels, using fileless attack methods or legitimate tools for malicious purposes. Effectively identifying and blocking these attacks requires the use of advanced detection methods such as analytics and machine learning.

Lastly, targeted attack groups increasingly leveraged living-off-the-land tactics in recent years because it allows attackers to maintain a low profile, by hiding their activity in a mass of legitimate processes. Targeted attack actors continued to pose a significant threat to organizations during 2018, with new groups emerging and existing groups continuing to refine their tools and tactics. The larger, more active attack groups appeared to step up their activity during 2018. The 20 most active groups targeted an average of 55 organizations over the past three years, up from 42 between 2015 and 2017. Many of these targeted attack groups consist of state-sponsored activities. Auspiciously, 2018 brought a significant increase in indictments in the U.S. against state-sponsored attack groups. Forty-nine individuals/organizations were indicted during 2018, up from four in 2017 and five in 2016. While most headlines were devoted to the indictment of 18 Russian agents, most of whom were charged with involvement in attacks relating to the 2016 presidential election, the indictments were far more wide ranging. Alongside the Russian nationals, 19 Chinese, 11 Iranians, and 1 North Korean individuals/organizations were charged.[xxiv]

Legacy Systems

Another carryover from last year's OCDC report, the prevalence of legacy (old) software and hardware systems in the U.S. and abroad presents a wealth of cybersecurity concerns. It is estimated that almost 4 percent (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.[xxv] 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.[xxvi] Lastly, legacy systems often hinder the sharing of information between systems on the same network; this creates data silos that cannot be accessed easily and cannot be backed up effectively.

Cyber Threat Summary

Year-to-year the cyber threat landscape appears substantively similar from the prior; however, every facet of cybercrime and cybersecurity is in a state of continuous evolution, an evolution that requires proactive solutions. The challenge of training enough personnel to join the ranks of cybersecurity continues. The type of attacks change year to year, and criminals continue to evolve in who they choose to attack and the methodologies they employ for their crimes. Cybersecurity is not becoming easier. From the private sector to the public, the impact of cybercrime is growing exponentially; the cost of cyberattacks spiked more than $1.5 million in the past year, going from $3 million per incident in 2018 to $4.6 million in 2019.[xxvii] With that growth, organizations and individuals must be proactive in their cybersecurity planning, training, and reporting or face the potential consequences.

Goals and Objectives

Incident Response Maturity

In 2018, OCDC collaborated 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. OCDC is committed to continuously advancing and maturing the ESF capability to ensure cybersecurity incident management best practices are leveraged and available when needed most. This objective includes incorporating and planning for upcoming political subdivision incident response planning, to ensure the state is well-positioned to support local needs.

Unified Communication Framework

Over the last year, a number of stakeholders have expressed an interest in an improved and unified communication plan, specifically to support cybersecurity. While several communication mechanisms currently exist and are utilized effectively, the need to shift to a more mature communication process is evident. For these reasons, OCDC will develop a multi-faceted communication framework to meet the demand of our stakeholders. The framework will encompass elements of day-to-day information sharing – both sensitive and non-sensitive – ad hoc support requests, cyber incident response, and management needs.

Education, Education, 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. Most notably, when discussing cybersecurity with the average (non-technical) person, they generally struggle to understand the 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. This issue is problematic for a variety of reasons – and represents the reason why this issue remains a continued goal.

Moreover, education, in relation to training and workforce development, will continue as an important issue for OCDC. According to cyberseek.org, the cybersecurity workforce labor shortage in the U.S. has eclipsed 300,000 open jobs – approximately 2,000 of which are in Nevada.[xxviii] The ability to secure information systems, address gaps, and generate improvements in cybersecurity hinges on a properly trained and available workforce – which currently does not exist. OCDC will make every effort to advance cybersecurity workforce development, as able.

Cultural Change

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 also raised awareness of the cyber threat significantly. OCDC aims to continue educating the community on the social 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 transform, and with a limited number of mature cybersecurity programs in Nevada – 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 our communities.

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. 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.

"It takes 20 years to build a reputation and a few minutes of a cyber-incident to ruin it" – Stephanie Nappo, Global Chief Information Security Officer – Societe Generale International Banking

Sources

[i] https://www.radware.com/newsevents/pressreleases/c-suite-2019
[ii] https://cybersecurityventures.com/cybersecurity-market-report/
[iii] https://cybersecurityventures.com/cybersecurity-market-report/
[iv] https://www.wired.com/story/election-security-2020/
[v] https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy
[vi] https://www.herjavecgroup.com/cybercrime-report-2017/
[vii] https://enterprise.verizon.com/resources/reports/dbir/
[viii] https://www.varonis.com/blog/cybersecurity-statistics/
[ix] https://blog.trendmicro.com/forecasting-the-future-of-ransomware/
[x] https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
[xi] https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
[xii] https://www.recordedfuture.com/state-local-government-ransomware-attacks/
[xiii] https://www.recordedfuture.com/state-local-government-ransomware-attacks/
[xiv] https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf
[xv] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
[xvi] https://enterprise.verizon.com/resources/reports/dbir/
[xvii] https://enterprise.verizon.com/resources/reports/dbir/
[xviii] https://enterprise.verizon.com/resources/reports/dbir/
[xix] https://www.csoonline.com/article/3341317/data-breaches-exposed-5-billion-records-in-2018.html
[xx] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/
[xxi] https://www.upguard.com/breaches/facebook-user-data-leak
[xxii] https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/
[xxiii] https://www.cnet.com/news/exactis-340-million-people-may-have-been-exposed-in-bigger-breach-than-equifax/
[xxiv] https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
[xxv] https://www.csoonline.com/article/2139382/data-protection/forgotten-risks-hide-in-legacy-systems.html
[xxvi] https://www.alvareztg.com/the-risks-of-outdated-technology-why-legacy-systems-cost-you-more-than-you-realize/
[xxvii] https://www.radware.com/newsevents/pressreleases/c-suite-2019
[xxviii] https://www.cyberseek.org/