ORANGE COUNTY'S DIGITAL DATA:
IS IT PROTECTED FROM CYBER ATTACK?

Table of Contents

SUMMARY **3**

REASON FOR THE STUDY **3**

METHOD OF STUDY **4**

BACKGROUND AND FACTS **4**

The Digital Environment **4**

Nature and Sources of Cyber Risk in Orange County **5**

Public Sector Initiatives to Combat Cyber Attacks **5**

Orange County Cybersecurity Defenses **6**

Executive Support ***6***
Physical Security Management ***8***
Digital Security Management ***9***
Mobile Device Security Management ***12***
Collaboration ***13***
Third Party Vendor Management ***15***
Administration ***15***
Risk Mitigation ***18***

CONCLUSION **20**

FINDINGS **20**

RECOMMENDATIONS **21**

REQUIRED RESPONSES **23**

REFERENCES **25**

APPENDICES **28**

Appendix A: Sources of Cybersecurity Standards and Best Practices **28**

Appendix B: Types of Cyber Attacks **31**

Appendix C: Orange County Information Technology Oversight Bodies **34**

SUMMARY

Today, for better or worse, we live in a digital world, and cybersecurity has become a household word. Information that defines our identity, health, finances, communications, and personal and commercial transactions is all saved on computers connected to the internet. Sensitive information is subject to attack and damaging use by hackers, criminals and even other nations. Many devices that control our public utilities and household systems are being exploited by malicious parties. The most recent example of cyber threat is the May 2017 WannaCry virus that used a Windows vulnerability to infect and encrypt files in thousands of computers in 150 countries. Affected systems included hospitals, railway networks, banks, automakers, and telephone companies.

Orange County is in the forefront of cybersecurity defense in many areas but there is still much work that needs to be done. One of the five California fusion centers (information sharing entity representing local, state and national agencies) devoted to identifying and issuing alerts on cybersecurity threats is located in the county. To further its cybersecurity initiatives, the county has both a seasoned chief information security officer (CISO) and an experienced county privacy officer (CPO) in place within the Orange County Information Technology department (OCIT), and has a firewall-protected centralized network configured to prevent the spread of malicious attack, as well as centralized email monitoring. Anti-virus protection and data backup programs are installed in most county agencies, all of which would welcome a central repository of cybersecurity alerts, best practices, firewall rules, procedural templates and early threat notifications.

There are also a number of county cybersecurity initiatives in development which show promise. With the full support of the Orange County Board of Supervisors (BOS), elected and appointed agency heads, and well trained county staff, county data and systems can remain protected and functional.

REASON FOR THE STUDY

The security and reliability of Orange County's digital information and information systems is critical to the ongoing efficient and effective functioning of county government and the protection of its citizens. Cyber threats to government and private information, as well as systems and associated digital data are in the news daily and of increasing concern.

Unfortunately, cybersecurity breaches are becoming more common and the personal, financial and reputational impact can be severe. In the past year, Orange County experienced a successful cyber attack involving the penetration of the Orange County Transit Authority (OCTA) systems through a third-party vendor. This resulted in the encryption of valuable data, a ransom demand for its return, permanent loss of some irreplaceable data, and an expense in excess of $700,000 to recover data and restore systems.

An additional breach occurred in which the confidential information, including member names, demographic information, Social Security numbers and other health plan details of about 56,000 CalOptima members may have been accessed. It is no longer a matter of *if*, but *when* an organization will experience a cybersecurity breach (NIST, 2012).

Due to the seriousness of the threats, the 2016-2017 Orange County Grand Jury's (OCGJ) investigation explored the extent to which OCIT and other county entities responsible for information systems and digital data have identified cybersecurity threats and instituted comprehensive security procedures.

METHOD OF STUDY

The 2016-2017 OCGJ interviewed 31 employees of the county, including both management and staff, in some cases multiple times. These included senior officials in the offices of the chief executive officer (CEO), OCIT, and those with elected heads, as well as people in charge of information technology and cybersecurity in most county agencies. To validate information and ensure depth of understanding across the county, we also interviewed certain employees of special districts, chosen for the critical nature of their digital data. The OCGJ also interviewed a selection of key city officials, chosen to represent both larger and smaller cities, as well as some deemed particularly vulnerable to cyber threats.

County documents relating to cybersecurity from multiple government entities were reviewed, including audit and testing reports, training records, strategic plans, information technology policies and standard operating procedures. The OCGJ also conducted thorough literature searches regarding cybersecurity in the government sector and reviewed national directives and material from standards-setting organizations on the subject. Current cybersecurity standards and best practices from respected sources were reviewed, including the framework from the National Institute for Standards and Technology (NIST), standards from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (ISO/IEC), and the Department of Homeland Security (DHS) communications (Appendix A).

BACKGROUND AND FACTS

The Digital Environment

Cybersecurity is the ability to protect or defend the use of cyberspace from cyber attacks. (Appendix B details typical types of cyber attacks.) This applies to personal use by an individual as well as an organization's use of the internet, and typically encompasses people, processes and technologies. Cybersecurity focuses on how to protect the confidentiality, integrity and availability of information from unauthorized access, modification or disruption (NIST, 2016).

For purposes of this report, a cybersecurity incident is an event that compromises the confidentiality, integrity or availability of an information asset; a cybersecurity breach is an incident that results in the confirmed—not just potential—disclosure of data to an unauthorized party (Verizon, 2016).

There can be significant costs connected to a cybersecurity breach. The recent Target settlement of $18.5 million with the states over its 2013 data breach (Masunga, 2017) is just one example,

but damage to an organization's reputation and credibility is also one of the biggest potential costs to an organization, because a cyber breach means lost business and requires action to regain trust (Ponemon Institute, 2016).

Nature and Sources of Cyber Risk in Orange County

Orange County has a great deal of potentially sensitive information stored on or accessed by its various digital systems. The volume of this information can be very large, giving rise to high levels of potential risk in the case of a breach. The type of information is varied and includes:

- Personal identification information, such as social security numbers, names and addresses.
- Personal health information and confidential medical records.
- Personal credit information such as names, credit card numbers and expiration dates.
- Law enforcement information including data about juveniles, sexual offenders, arrest records and jail management.
- Child Welfare System records.
- California Aid and Family Support information.
- Data on pending criminal and civil litigation.
- Building permits and county property records.
- County investment portfolio information.

Data on any county device connected to the internet is at risk from a variety of potential attackers such as criminals, hackers, hacktivists, nation-state actors and even organization insiders. These malicious agents are pervasive, persistent and agile. Over 2,642 total data breaches have occurred across public and private organizations from 2010 to 2016 (Privacy Rights Clearinghouse, 2017). Advanced cyber attacks can go undetected for approximately 200 days on average, allowing cyber criminals ample time to harvest sensitive data, including passwords and other credentials to be used in subsequent attacks following the initial breach (Microsoft, 2016).

No one is immune. All county organizations need to determine what their high-risk assets consist of, who controls them, and who makes informed decisions as to how much risk the organization is willing to incur, balancing the benefits of technology to satisfy user requirements against keeping sensitive data secure.

In 2015, the public sector accounted for 74% of all reported cyber incidents and 9% of reported breaches nationally (Verizon, 2016). Several Orange County government departments reported multiple sensitive privacy information breaches in 2016. The majority were fraudulent email incidents, all of which were contained. There were nine reported incidents involving county systems in 2015 and the first half of 2016. Two widely published breaches involving other county governmental entities, the OCTA and CalOptima, occurred in 2016.

Public Sector Initiatives to Combat Cyber Attacks

As the focus on cybersecurity has increased in response to an increasing number of incidents and breaches over recent years, all levels of the public sector have ramped up their cybersecurity activity. At the federal level, the Cybersecurity Act of 2015 provided important tools necessary

to strengthen the nation's cybersecurity, making it easier for government entities such as the County of Orange and private companies to share cyber threat information with each other.

Part of this effort was the establishment of fusion centers, owned and operated by state and local government and supported by the DHS's Office of Intelligence and Analysis and the Federal Emergency Management Agency, providing these multi-agency centers with resources, training, and other coordinated services. The collaborative nature of these government entities maximizes their ability to detect, prevent, investigate and respond to criminal and terrorist activity. Located in primarily major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health and other local entities to lawfully gather and share threat-related information. One of California's five fusion centers, the Orange County Intelligence Assessment Center (OCIAC), is located in Orange County and provides cybersecurity alerts and information to OCIT.

In 2016, California state assembly bill 1841 mandated that cybersecurity incident response standards be included in each state agency's technology recovery plan. Orange County has included the development of a centralized incident response plan template in OCIT's five year cybersecurity "roadmap." A beta version of this incident response plan is currently under review by the Orange County Cybersecurity Joint Task Force.

Orange County Cybersecurity Defenses

Cybersecurity vulnerabilities are produced by weaknesses in technology (operating systems, applications and tools) and people (training and awareness). Large organizations such as the County of Orange are faced with maintaining complex systems that have evolved over time. For example, OCIT alone supports over 630 servers across more than 38 locations and manages over 80 routers, 380 switches, 42 wireless bridges and 173 wireless access points across 83 locations in addition to a large number of laptop and desktop computers and over 100 software applications for various county agencies (Orange County Information Technology, 2017). All of these systems and devices, plus many more government devices not under OCIT's control, must all be maintained and protected from cyber attack.

Key areas of cybersecurity defense for Orange County are described in detail in the following sections.

Executive Support

County Board of Supervisors

Support from top management is critical to the success of any cybersecurity program. Highlighting the importance of board and executive level support, the 2017 update of the National Association of Corporate Directors (National Association of Corporate Directors, 2017) cyber risk oversight handbook includes the following five recommendations for boards of directors:

- Approach cybersecurity as an enterprise-wide risk management issue, not just an information technology issue.
- Understand the legal implications of cyber risks.

- Boards should have adequate access to cybersecurity expertise; cyber risk management should be given adequate time on board agendas.
- Directors should set expectations that management will establish an enterprise cyber risk management framework.
- Boards need to discuss details of cyber risk management.

The OCGJ found that the BOS has heightened awareness of cybersecurity threats and is very supportive of cybersecurity efforts, partly given the 2016 OCTA ransomware incident, which had a significant and widely publicized impact. County executives are leading efforts to provide centralized support for countywide cybersecurity efforts and, with other county leaders, recognize the sensitivity and vulnerability of the digital information the county manages. The BOS and county CEO recently supported the deployment of mandatory annual online cybersecurity awareness training for all county employees, including the BOS staff. Initiated in 2017, this training also includes mandatory review by each employee of the county IT use policy. Mandatory two-hour biennial fraud training provided by the county district attorney (DA) and auditor-controller was instituted in 2016.

Funding

A key indicator of executive support is the amount of funding allocated to the effort. In 2016, an OCIT request for a $98,000 comprehensive ("defense-in-depth") cybersecurity initiative was not approved. For the fiscal year ending 2017, however, the budget for the CISO's group was increased from $1.8 million to $2.2 million to cover a specific cybersecurity project addressing zero-day infections (those that result from previously unknown vulnerabilities). A contract was recently awarded by the BOS to an outside vendor for a countywide cybersecurity vulnerability assessment program. The BOS approved the $2.5 million cost of the assessment program and requested that all county departments and agencies complete assessments by June 30, 2018.

The Grand Jury had difficulty identifying financial commitments to cybersecurity across all county agencies and departments, as cybersecurity is not currently split out as a separate line item in county information technology (IT) budgets. Cybersecurity budget requests are approved as part of overall IT requests and are basically responsive to perceived immediate cybersecurity threats.

Cybersecurity Strategic Planning

Most county agencies and departments do not appear to have any cybersecurity strategic plans in place. No current OCIT cybersecurity strategic plan exists, but cybersecurity is part of the broader IT strategy. The OCIT Enterprise Security group is currently working on a five year cybersecurity strategic plan and has developed a tentative five-year roadmap for cybersecurity which could develop into a strategic plan at some point in the future. Plan elements include county programs for cybersecurity auditing and assessment, policies and procedures, training and updating various hardware and software cybersecurity defenses. It is important to note that many of the items on the roadmap are not yet approved or budgeted by the BOS, therefore implementation and timing of these programs is tenuous.

The IT Cybersecurity Joint Task Force, recently formed and headed by the county CEO, is a key entity for accomplishing cybersecurity planning, in part by creating a county cybersecurity policy manual that would apply to all departments. The policy manual completion is expected in March 2018. Approval is slow because the county process requires review by all stakeholders, including county counsel, the county CEO, unions, administrative services, risk management and others. With the cyber threat landscape changing constantly, counties are as much as 10 years behind the federal government, and cities 10 years behind the counties in their implementation of current best practice cybersecurity measures, according to OCIT.

Oversight

It is common for government entities to set up oversight bodies for important projects and programs. There are several such IT entities that oversee, review, advise and inform on cybersecurity efforts in county agencies and departments.

Examples of cybersecurity oversight at the Orange County department and agency level include:

- The Sheriff's cybercrimes unit, which handles cybersecurity oversight for the Sheriff's department.
- The DA's cybercrime investigation unit is headed by a supervising investigator, who handles cybersecurity oversight for the office. However, the unit currently only has one analyst, who is on loan to another agency. Staffing plans for this group envision growth to five analysts, but this is dependent on funding.

The OCGJ found no evidence of any other regularly scheduled reviews of cybersecurity procedures and readiness, so it is unclear how much oversight or even discussion of cybersecurity matters occurs at the departmental level.

Physical Security Management

The management of physical assets, such as facilities, servers, network equipment, PCs and mobile devices, is an important component of cybersecurity, including safeguarding access to digital equipment and data, as well as the safe return of intact data from employees leaving county service or transferring between county departments.

When under physical control of management, equipment with digital data can be more easily subject to cybersecurity controls. The county uses a number of physical entry and exit controls, including guarded entry points, key cards and combination locks on doors to sensitive areas. At the Registrar of Voters (ROV), for example, all these physical security measures are in use, as well as voting equipment seals and tags.

A growing number of employees conduct county business with county smartphones, tablets and laptops, posing several security concerns. For example, the practice of issuing devices to users rather than departments becomes a potential cybersecurity issue when individuals transfer between county departments taking their mobile devices with them. Other mobile management issues include device theft; a need for consistent policies across departments and agencies, and

the large number of different devices and operating systems in use across the county. This all makes the protection of digital privacy data and timely updating of mobile operating systems and applications a complex and problematic effort.

In addition, some county digital assets are housed outside the county. For example, the local nonemergency government 311 phone services data are located on a server in the Midwest. The county also maintains a secure offsite location for long term data backup with a data storage company. The county is considering requiring that data that is stored on third party servers in the cloud be housed only within the U.S. by cloud service providers accredited by the Federal Risk and Authorization Management Program (FedRamp). FedRamp is a government-wide program providing a standardized approach to security assessment, authorization and continuous monitoring, meeting federal cybersecurity standards for cloud products and services. Certification of cloud services by this body provides confidence in the data security of third party cloud service vendors.

Some Orange County agencies and departments have employee exit procedures that reflect best cybersecurity practices, but none are comprehensive. For example, the county revokes access on exit and retrieves all county devices, but does not currently do a comprehensive check of USB drives and other devices having storage capability, prior to their re-use, scrap or sale. To avoid data breaches when equipment is lost or stolen, all sensitive data or, better yet, entire hard drives should be encrypted.

Sensitive digital personal health information was removed on a USB drive from an Orange County government entity in 2016. The county is currently reviewing its employee exit processes, which are now managed and enforced by human resources staff assigned to individual agencies.

Digital Security Management

The Centralized County Network

The county network is the first layer of defense against cyberattack. Aspects of network cybersecurity defense include:

- Firewalls and email traffic monitoring systems.
- Regular maintenance and review of logs.
- Routers with passive vulnerability scanners.

Aspects of effective cybersecurity defense that apply to all county digital devices include:

- Monitoring of outbound traffic as well as inbound traffic for suspicious activity.
- Regular and timely patching ("bug fixes") of software and operating systems.
- Regular and timely updating (installing new versions) of software and operating systems.

The county's centralized network is segmented with multiple firewalls to prevent the spread of any malware, and uses intrusion detection and email filtering systems to detect and deter malware from entering the network. The remaining departmental networks are generally

segmented and include some provision for intrusion detection. For example, an application for enterprise-wide visualization, alerting, reporting and real-time situational awareness, is used by the Sheriff's department to prevent network intrusion.

The county oversees the county network support vendorto ensure the vendor follows contractual service level agreements, conducts monthly testing and provides both monthly and quarterly reports on network security status. In addition, the county has the contractual right to conduct annual audits of the vendor's service levels and security activities. This vendor conducted penetration testing and a security assessment of the OCIT network in 2016. OCIT is considering future implementation of network-based data loss prevention technology, which would monitor all traffic leaving the network and provide immediate alerts of any potential loss of sensitive information, but this has not yet been approved or funded. Monitoring of email traffic using this technology is currently scheduled to be implemented by fall of 2017. This is an important step in detecting and preventing, or at least mitigating, a cyber breach. A physical device currently monitors and logs incoming traffic on the county network for suspicious activity and issues alerts, which have resulted in mitigating cyber attacks. However, the volume of data is so large that the logged traffic data is difficult to analyze in a timely fashion. The device can only hold approximately two weeks' worth of data and the presence of dormant malware can go undetected for over a year, if not identified in the first two weeks.

County Websites and Internet Access

County public websites are typically air gapped (not connected to the internal county network) to prevent cyber attacks. A web filtering system is also used to control access to questionable or problematic web sites that are accessed through the county network by county employees (end users).

Cybersecurity Defense for County Endpoints (Computers, Laptops, and Tablets)

The third party vendor that manages the county desktop support services and service desk services and is contractually obligated to issue monthly status reports, service level assessments and regular vulnerability assessment audits. In addition, vendor service level requirements are reviewed at the end of each contract year for possible improvement.

OCIT is currently in the process of making advanced threat protection available for email for countywide computers. This software identifies and strips dangerous contents, such as hyperlinks, from emails before they reach county employees.

The county is also looking at using regional cooperative agreements (RCAs) for anti-virus software, as well as for more sophisticated endpoint protection software that addresses as-yet-unknown malware. An RCA negotiated by OCIT would allow departments, agencies or other countywide government entities to acquire software much more efficiently without conducting a separate request for proposal (RFP) process. OCIT is also considering implementing computer-based data loss prevention technology, which would block the loss of sensitive privacy information from files and attachments on user workstations as well as from the network.

Several individual county agencies have also taken steps to improve cybersecurity. For example, the Health Care Agency (HCA) recently purchased a user "sandbox" system (secure and contained) to detect and arrest malware. The Sheriff's department mobile units are now password protected and data is encrypted in transit. At least one county agency is moving to full disc encryption on all laptops for maximum protection from loss or theft.

Password Management for All County Devices

Weak, default or stolen passwords accounted for 63% of confirmed data breaches in 2015 (Verizon, 2016). The increasing use of email addresses instead of more unique user names or passwords is exposing an even greater number of users to attack (Phishlabs, 2017). Best practices recommend regular password maintenance and the use of multi-factor authentication. Multi-factor authentication includes, in addition to a strong password, an additional layer of user-unique information, which could include physical access tokens or biometrics, e.g., fingerprints. Different passwords for each application and system the user accesses are generally recommended in order to limit vulnerability when one system or application is compromised.

The county does not currently mandate multi-factor authentication on county endpoints, such as workstations, laptops, tablets and smartphones and password management is typically under the control of the end user, rather than the organization. Employees who connect to county systems remotely, however, use encrypted access to the county Virtual Private Network (VPN) using multi-factor authentication with a token or a special numeric code.

Patch and Update Management

Over 80% of cybersecurity incidents are thought to stem from the exploitation of known vulnerabilities (Verizon, 2016). The timely and complete installation of patches and updates as they are released by vendors is therefore key to maintaining cybersecurity endpoints. This was highlighted by the WannaCry virus attack in May 2017. At the time of the attack, the Windows vulnerability was known and a patch for Windows was available but, in spite of this, over 200,000 servers and computers in over 150 countries were infected. This suggests that organizations are slow to patch significant vulnerabilities. As vulnerabilities are identified by manufacturers or users, including "white hat" (friendly) researchers, vendors issue patches to their applications and operating systems that eliminate these access points. Instituting preventive measures, such as patching and version updates, promptly are therefore more valuable than increased vulnerability testing (SANS Institute, 2017).

County agencies and departments often resist system downtime necessary to install patches, but most conduct nightly user data backup to mitigate the potential impact of a breach. While timely backup can be effective against "phishing" attacks (those that gain access through fraudulent emails) the backup itself can become corrupted if the attack is not discovered in time.

In a recent shared services pilot report, OCIT noted that there were over 60 different endpoint operating system configurations in use just in the pilot group. This is another indication of the diversity that exists in the county that makes timely patching and updating of county endpoints

difficult. In 2017, OCIT developed and received approval for consistent guidelines for this pilot group as to when and how county computers receive patches and updates (Orange County Information Technology, 2017).

Data Encryption

Data encryption (encoding) of sensitive data is a very effective defense against cyber attack, especially in the case of mobile devices. Data encryption safeguards data even if a hacker successfully penetrates county systems or comes into possession of a mobile device that contains sensitive data. The encrypted data is useless to them without the access key. Encryption of county data across agencies is not consistent, but may not be required, depending on the nature of the information and the risk associated with its loss. Currently, some data stored at the IT Data Center (e.g., HCA data) on dedicated servers is encrypted, and at least two agencies, the HCA and Social Services Agency (SSA), are moving to full disk encryption on all laptops. OCIT is also including implementation of both at rest and in transmission encryption of sensitive data in the county's formative 5-year cybersecurity roadmap.

New Cyber Defense Tools

Application of artificial intelligence and machine learning (ML) technologies to cybersecurity has been identified as one of five key cyber trends for 2017 (Straight, 2017). OCIT is currently evaluating an ML endpoint anti-malware system which is promising for detecting new cyber threats. It includes identification of zero day vulnerabilities (so-called because they come to light when there are zero days to fix them) and a sandbox in which malicious websites, downloads, or attachments are isolated, keeping county data secure.

Typically this technology performs real-time monitoring, correlation and analysis of logged event data, and activity using advanced applied mathematical models to alert cybersecurity to suspicious items. In addition, ML can be used to identify previously un-encountered threats that would otherwise go undetected.

Mobile Device Security Management

The use of mobile devices (smartphones, tablets) are becoming universal and can pose their own unique security challenges to an organization. Various protective measures can be deployed to mitigate the risk of a breach through mobile devices, including:

- Robust access control, including two-factor password authentication and biometrics.
- Encryption.
- Automated backup.
- Remote "find and wipe" tools that search for and destroy malicious files.
- Regular and timely updating of the operating system.
- The installation of applications only from trusted sources.
- Denying "jailbreaking," which removes manufacturer or carrier restrictions on mobile devices.
- Regular and timely updating of applications.
- Regular maintenance of all third-party passwords.

- Awareness of phishing emails or alerts.

While the county uses a VPN and secure File Transfer Protocol (FTP) for external communications and data transfer, mobile devices may be compromised in several ways. When employees transfer between departments, they currently may take their county-issued mobile devices with them without any IT review. Also, mobile devices, their operating systems, and their applications are currently not patched and updated in a timely fashion. Mobile devices, of which there are many in county government, are particularly subject to theft and subject to different policies across departments and agencies. Most departments are using mobile device management software, but this is not centralized or standardized as yet, and many devices are not currently registered in the management software and so are not currently included.

Collaboration

Collaboration has been the cornerstone of federal and state strategies for strengthening the nation's cybersecurity. Orange County is fortunate to have one of the five California fusion centers in the state, activating the collective strategy. Implementing collaboration at the local level, however, has been mixed.

Part of OCIT's mission is to foster a work environment that values collaboration and teamwork and leverages the diverse skills and experiences of the organization, but this is challenging with 22 different agencies, particularly from a technology standpoint (Orange County Information Technology, 2017). OCIT's authority only extends to appointed department heads and arises through the support of the CEO and the BOS. County government entities generally operate independently of the BOS, however, supervisors often sit on the entities' governing boards. These independent entities include elected agency executives, who have complete authority over the function of their departments with the exception of budget issues; Joint Power Authorities (JPA); city governments; special districts; and school districts. The actual cybersecurity effort is focused at the county department and agency level and is heavily dependent on the number of staff and funds available in a given entity.

Information technology departments across the county have operated using a decentralized model since 1996, with agencies independently staffing personnel and procuring products and services. This has resulted in reliance on systems using outdated technology; inconsistent and inadequate security standards, policies and training; and low levels of cross-agency collaboration and teamwork (Orange County Information Technology, 2017). County departments and agencies are generally very concerned with end user convenience and achieving business goals and are reluctant to accept what they perceive as a one-size-fits-all approach to cybersecurity. For example, the OCGJ heard that stringent network filtering was responsible for slower response times and user dissatisfaction. Departments feel that centralized alert notification, vulnerability, penetration testing, policies, procedures and standards, while helpful in some respects, should be individually tailored to enable rather than restrict the unique business of the department. OCIT is sensitive to these concerns. For example, an exception procedure is proposed within standardized county cybersecurity policies and procedures to accommodate individual departmental business needs. In addition, the county Technology Council meets

bimonthly to identify and recommend business process improvements and facilitate agencies' collaboration on cybersecurity.

The cybersecurity joint task force of the county IT Executive Council, representing OCIT, the county counsel, county risk management and several departmental administrative services, facilitates collaboration and visibility of countywide efforts, meeting monthly to jointly develop best-practices-based policies and procedures.

In general, county departments and agencies are interested in receiving timely information about cybersecurity, but there are currently only a few avenues to do so. Most departments tend to collaborate with similar agencies but do not actively seek out and collaborate with OCIT. Some agencies and departments, including the Public Defender, HCA and SSA, are beginning to collaborate with OCIT. Some county entities that have had the opportunity to foster cybersecurity collaboration between county groups include:

- The Cybersecurity Task Force: This body was established in April of 2017 with a goal of putting cybersecurity standards in place.
- The Cybersecurity Working Group: The original county bimonthly working group was not effective because it was not made up of decision makers and participation was not mandatory; it was discontinued in 2016.

To foster collaboration, awareness and visibility of cybersecurity issues, and adoption of best practice security activities and programs, OCIT staff attend meetings of other county government entities, including cities; are developing a cybersecurity website, scheduled to be available in the summer of 2017; make cybersecurity presentations to county department heads; and negotiate RCAs for cybersecurity products and services that allow all county government entities to use these products and services through sub-agreements without having to go through a separate RFP process.

Pooling resources to monitor cybersecurity alerts, ensure rapid alert dissemination, and share cybersecurity standards and best practices can reduce the resources required to effectively defend against cyber attack. Orange County currently collaborates with several government sources of cyber threat alerts, including:

- The Orange County Intelligence Assessment Center (OCIAC).
- The Multi-State Information Sharing and Analysis Center.
- The United States Computer Emergency Readiness Team.
- Homeland Security's FireEye Insight Portal, which includes unclassified alerts without identified sources.

Alerts and advisories are currently received by OCIT and sent out through the county's central public information office to all county departments and some cities. OCIT is working to put cybersecurity alerts on a new countywide cybersecurity portal as well. This portal was recently launched for use by county departments. In addition, OCIT distributes monthly summaries of threats directed at county systems.

Sharing of best practices and standards is welcomed by county government entities, but their application varies widely across county agencies and departments and ranges from the use of best practices and standards developed internally to those developed by national bodies, such as

NIST and Homeland Security. There are a number of national, state and regulatory bodies that provide cybersecurity standards and best practices (Appendix A).

Third Party Vendor Management

The county uses two main third party IT vendors. The county's agreements with these vendors for network maintenance and desktop support, respectively, mandate that they both purchase and maintain insurance that includes "Professional Errors or Omissions" coverage or "Cyber or Technology" and "Privacy Liability" coverage with a $20,000,000 limit.

Some of the most significant recent cyber attacks, such as the 2013 Target breach, resulting in very public consequences, originated with a third-party service provider (Chuang, 2017). In Orange County, the 2016 phishing attack on OCTA occurred through a third-party vendor and resulted in the loss of a large amount of data and significant recovery costs for the agency.

Best practice vendor management in the area of cybersecurity includes effective contract clauses with service level agreements covering cybersecurity documentation, response times, backup and recovery procedures; contractual provisions for auditing the vendor's security and their cybersecurity capabilities; and appropriate warrantees and indemnities. OCIT is currently working with procurement to review the cybersecurity contract language in clauses used in their third party IT vendor contracts, and is now part of the review process for select county contracts. The most recent county contract language requires that the county be provided with copies of vendor audits. The county is also considering including a requirement in RFP's for such vendors to have at least $1,000,000 in cybersecurity insurance. In the case of sole-source contracts through agencies, the county could be exposed in the event of a breach. OCIT is also urging the use of RCAs to ensure consistent application of best practices regarding vendor management, as well as to save resources across the county.

Administration

Documented Procedures

When a cybersecurity breach occurs, a rapid and effective response per a documented plan can be critical to mitigating the damage. This is especially important since the actual nature of the cyber threat may not be known in advance. The planned response to the incident must include stopping the attack and returning critical systems to operational status, as well as preserving the evidence to understand the attack and its origins. There are a number of good incident response plan templates published by organizations such as the U.S. Department of Justice (U.S. Department of Justice, 2015) and NIST.

Good incident response procedures include periodic testing, as well as practicing the plan internally and with vendors and partners using simulations and table-top exercises (ISO - ANSI, 2010). The county is currently working on the creation of a standard comprehensive incident response plan with an approved exception form to allow agencies to customize the plan for their specific regulatory requirements and needs. Once approved and implemented, the county intends to test the plan's effectiveness annually.

Training

The OCGJ heard from various sources that the highest and most persistent cybersecurity risks in the county are phishing attacks and lax end user practices. From November of 2016 to January of 2017, 66% of incoming county emails were identified as spam, phishing or virus laden. Only 34% were legitimate.

The county recently contracted with a third party vendor to provide cybersecurity training for county employees. This is an online, mandatory and customizable annual training program that covers ransomware, password guidelines, safe computing, social engineering, phishing, physical security, privacy, mobile devices, social media and malware. Any county entity, including the cities, can benefit from county pricing for this training program using a sub-agreement. The annual Cyber Security Awareness Training (CSAT) was implemented January 18, 2017, through a memorandum to all county employees from the CEO's office. Fully 89% of county employees with network access (5518 people) had completed the online training as of the publication of this report and full completion of the training requirements by all county employees is anticipated by the end of 2017.

Another example of countywide training that encompasses cybersecurity is the mandatory biennial two-hour fraud training program implemented in 2016 and conducted by the DA and Auditor-Controller.

At the department level, IT training that may include cybersecurity is currently provided by several third party vendors, and training materials have also been developed internally by department personnel. An example is the internal training by the ROV, which used internal training prior to the last election focused on phishing and vendor testing. Other county agencies also use outside third parties for training focused on specific areas, such as the HIPAA training conducted for the county by an insurance company. HCA, SSA, Sheriff, DA, Public Defender and ROV do the most cybersecurity-related training. The type and frequency of training varies widely in other county agencies and departments. Development of additional general employee and IT department cybersecurity training will take time due to the involvement of county unions and other stakeholders in the process.

The county would like a minimum level of IT cybersecurity training required for all county employees, to have cybersecurity management certified as Certified Information Systems Security Professionals, and for all department analysts to be qualified to handle cybersecurity incidents.

Periodic testing or auditing of training effectiveness is apparently not currently conducted by any county agencies or departments.

Cybersecurity Audits

The current contracts with the county's network support vendor and its desktop support services vendor have service level guarantees and provisions for county audits of vendor cybersecurity

procedures. However, currently there are no countywide standard operating procedures for the conduct of cybersecurity audits and assessments and most departments do not currently audit cybersecurity.

An OCIT audit by the Auditor-Controller's office that includes cybersecurity, which is scheduled for 2017, is expected to include a review of countywide cybersecurity risk assessments that were recently contracted by OCIT.

Likely to be hampering the county's audit efforts, the county Director of Performance Audit position is still vacant and the recruiting process is ongoing as of the date of publication of this report. A few individual agencies have their own audit programs. For example, SSA has its own internal security audit program in place and the ROV has an audit pending by an outside vendor. The CPO will be conducting a HIPAA audit at the HCA in 2017 and the Sheriff did a security audit in 2015. The DA, Sheriff and Probation department are also required by the Department of Justice (DOJ) to conduct annual audits in order to maintain access to DOJ systems.

Cybersecurity Testing Procedures

Currently there are no countywide standard operating procedures for the conduct of cybersecurity penetration testing (probing for computer or network vulnerabilities), nor for one-time compromise testing, and the OCGJ found that a minimal amount of cybersecurity testing or none at all is done at the department level.

The OCIT Data Center, through the county desktop services vendor, does monthly cybersecurity testing and did a penetration test and security assessment in 2016. Examples of testing at the agency level include 2014 and 2015 HCA application penetration tests and HCA currently conducts an annual risk assessment in accordance HIPAA. The Sheriff's department conducted a recent penetration test and conducts a real-world testing exercise twice a year. The ROV conducted a simulated election night cyber attack with OCIT prior to the last election.

As to vulnerability testing and assessments, the OCGJ was informed that current departmental assessment programs are embryonic except for HCA, which is required to have robust programs in place in compliance with HIPAA and as incentivized by the Health Information Technology for Economic and Clinical Health Act (HITECH), which strengthens HIPAA rules concerning the electronic transmission of health information.

Effective Cybersecurity Staffing

Staffing for cybersecurity in the county is a challenge shared across all public agencies. Approximately 43% of the county's current IT staff will be age-eligible for retirement within the next four years (Orange County Information Technology, 2017). The OCGJ were repeatedly told by those we interviewed that it is a challenge to staff cybersecurity positions. Demand for the cybersecurity skillset is high at all levels, outpacing the ability to train enough otherwise qualified IT employees. In addition, the job is often a high pressure position, dealing with crisis situations (Straight, 2017). Due to these factors, the hiring process in the county can take from 8 weeks to 8 months, depending on the background check and other requirements of the position. The county budget cycle can complicate and lengthen the hiring process considerably, if a hiring

freeze is put in place or a selected candidate does not accept the position and the process must be restarted. In some cases, though, cybersecurity positions have been filled using other departments' candidate lists to advance the process, though this tactic may result in less qualified and/or inexperienced hires.

The process of staffing cybersecurity positions can also be complicated by the rapid pace of change in the cybersecurity arena, leading to outdated county IT job classifications, resulting in descriptions and salary levels that do not keep pace with the private sector cybersecurity job market. Also, the state of current county compensation is not favorable compared with those available in the private sector. The fact that changes to job classifications and benefits must be negotiated with all stakeholders increases the time required to respond to market changes. All of the above make it particularly difficult for the smaller departments to effectively staff cybersecurity.

OCIT has a well-qualified and experienced chief information security officer (CISO) in place and a staff of six, with anticipated growth to eight. OCIT has recently added audit expertise that will assist in department cybersecurity self-assessments with the addition of a cyber resilience manager in its Enterprise Security Group, with the goal of reducing incident recovery times across the county. Staffing this audit position will require a certified cybersecurity auditor. OCIT also has a county privacy officer (CPO) in the cybersecurity group whose primary goal is to reduce breaches. The CISO has held the position for slightly over a year. The CPO has been part of OCIT for slightly over a year, having transferred from HCA.

IT staff at the agency and departmental level varies from one to over 100 IT employees and ranges from no cybersecurity support to four dedicated staff. The majority of the departments surveyed by the OCGJ use IT analysts supporting cybersecurity as part of their overall job assignment. It was suggested that it would be productive for each department to have a certified departmental information security officer (DISO) and that this could be a shared services position, making it possible for smaller departments to use only the amount of DISO resources that they need.

Risk Mitigation

Risk Assessment

Per best practices, after assessing cyber vulnerabilities, county agencies and departments must identify and decide what level of business risk each will accept. Risk assessment includes both identifying what information is sensitive and what level of protection is required. An organization must also know what sensitive information vendor partners store and have access to, who is responsible for it, as well as where it is kept. NIST provides a methodology for inventorying information, determining the likelihood of an incident and prioritizing necessary action (NIST, 2016).

A 2014 audit by a national auditing firm noted that the county did not have any formal enterprise risk management program in place (Plante Moran, 2014) and the OCGJ did not find any formal countywide risk assessment and management programs in place. Several county departments

indicated their cybersecurity goal was risk mitigation, not risk avoidance, but a majority indicated that their goal is to have no cyber incidents or breaches.

On April 11, 2017, a consulting firm was approved by the BOS to conduct baseline security assessments for all county departments, including those with elected heads, and departments are directed to complete these assessments by June of 2018. It is anticipated that this project will include assessments in all critical areas of cybersecurity, including the host (computer and server), network devices, network mapping and traffic analysis, and a review of cybersecurity policies, processes and procedures, including physical security. The BOS directed OCIT to provide a written report on the state of county cybersecurity on a bi-annual basis, starting November 14, 2017. Publicizing the trending information on the most common and dangerous vulnerabilities to county data and information systems, plus the completion status of departmental assessments, are expected to motivate departments to use cybersecurity product and service RCAs to strengthen their cybersecurity. The county is also evaluating the possibility of renegotiating or rebidding existing cybersecurity contracts for other products and services to set up additional RCAs.

The county agencies with digital data of highest risk were identified as being:

- HCA, due to the large amount of personal health information;
- SSA, due to the type of information, number of records kept and length of time retained;
- Assessor, due to building permit and property ownership plus payment information;
- Any department that keeps digital personally identifiable information; and
- All departments in the case of mobile device loss.

Insurance Protection

Having a cybersecurity insurance policy is a key part of an organization's risk management arsenal. Insurance can mitigate many of the costs of a cybersecurity breach, such as:

- The cost of forensic investigation to determine the cause of the breach and how to prevent a reoccurrence.
- Notification of affected individuals.
- Identity monitoring by an outside organization, typically with periodic reporting to individuals whose information has been compromised.
- Legal costs.

The county currently has a cyber insurance policy with $25 million in coverage for each claim as well as in the aggregate, and a $250,000 deductible. The amount of coverage is driven in large part by the available budget. This policy covers network security, media, privacy and regulatory liability, data breaches, business interruption, data recovery and cyber extortion. While this amount was deemed sufficient by the county to cover a single agency breach, it may not be sufficient for a massive breach across multiple agencies where costs are driven by the amount of sensitive information compromised. The OCGJ was told the average cost per breach, at least in one government entity, could be $200 per identity compromised. Using HCA as an example, 100,000 patient records could be exposed in a breach, resulting in a cost of $20 million. The

OCGJ was informed that in the very unlikely case of a massive breech involving 100% of the county's records, the cost could reach $1 billion.

CONCLUSION

Maintaining cybersecurity in Orange County's multifaceted government is a complex challenge. Information that defines citizens' identity, health, finances, communications, and personal and commercial transactions is all saved on computers connected to the internet or stored in the cloud and is subject to cyber attack. The resources allocated to cybersecurity are determined by the degree of risk the county is willing to assume.

To further its cybersecurity initiatives, the county has a number of oversight bodies, an Enterprise Security Group with an experienced CISO, CPO and staff; a firewall-protected centralized network with email monitoring and intrusion protection. Anti-virus endpoint protection and data backup programs are in place in most county departments and agencies as well. There are also a number of county cybersecurity initiatives in development.

The county can draw from many national and state government cybersecurity bodies and programs to leverage its efforts. One of five California multiagency fusion centers devoted to identifying and issuing cybersecurity threat alerts is located in Orange County.

Although much has been done, the OCGJ has identified areas for further work to sufficiently protect county information. This requires sustained support by the BOS, as well as elected and appointed agency heads. Areas of need include countywide risk assessment and mitigation, trained cybersecurity staff, digital security management, increased collaboration countywide, third-party vendor management, and documented centralized procedures.

FINDINGS

In accordance with *California Penal Code Sections* §933 and §933.05, the 2016-2017 Grand Jury requires (or, as noted, requests) responses from each agency affected by the findings presented in this section. The responses are to be submitted to the Presiding Judge of the Superior Court.

Based on its investigation titled "*Orange County's Digital Data: Is It Protected from Cyber Attack?*" the 2016-2017 Orange County Grand Jury has arrived at eight principal findings, as follows:

F.1. Orange County government entities are prime cyber targets, under constant cyber attack, and both public and private information held by these entities are not adequately protected.

F.2. The county is subject to many types of cyber attacks but phishing currently represents the highest risk to the county's sensitive information.

F.3. Some county cyber attacks come through third-party vendors, who may not always be sufficiently protected.

F.4. The county has taken a number of steps to safeguard its digital data and systems against cyber attack, but there are a number of actions generally recognized as cybersecurity best practices that still need to be implemented.

F.5. County financial records do not separate out cybersecurity as a line item, making it hard to determine what resources are being allocated in the area and therefore what additional funds are needed.

F.6. Cooperation among county agencies is currently limited due to organizational and cultural issues including the visibility of available centralized OCIT cybersecurity support, the inward focus of county agencies and the fact that the influence of the BOS to compel collaboration is largely limited to county agencies with appointed heads that report to the county CEO and, to a lesser degree, the county agencies with elected heads.

F.7. OCIT has an effective team in place for addressing cybersecurity deficiencies, but is only in the formative stages of implementing centralized standards and best practices for cybersecurity. Outside OCIT's control, county government agencies are taking advantage of the county's cybersecurity initiatives to different degrees.

F.8. IT employees across county government are largely untrained and uncertified in cybersecurity, especially at the agency level. Staffing for cybersecurity is challenging due to outdated county cybersecurity job classifications and salary levels, as well as lengthy county hiring processes, particularly for those agencies requiring extensive background checks.

Penal Code §933 and §933.05 require governing bodies and elected officials to which a report is directed to respond to findings and recommendations. Responses are requested from departments of local agencies and their non-elected department heads.

RECOMMENDATIONS

In accordance with California Penal Code Sections §933 and §933.05, the 2016-2017 Grand Jury requires (or, as noted, requests) responses from each agency affected by the recommendations presented in this section. The responses are to be submitted to the Presiding Judge of the Superior Court.
Based on its investigation "*Orange County's Digital Data: Is It Protected from Cyber Attack?*" the 2016-2017 Orange County Grand Jury makes the following 18 recommendations:

R.1. The county should establish a periodic cybersecurity audit schedule for all third-party vendors that connect to county networks and systems by 12/31/2017.

R.2. OCIT should select, acquire and direct the implementation of computer-based data loss prevention capability by 12/31/2017.

R.3. The county should review, update and standardize all employee and contractor exit procedures to ensure the security of countywide sensitive information by 12/31/2017.

R.4. OCIT should establish a countywide cybersecurity working group by 12/31/2017. Participation should be mandatory for County of Orange agencies that report to the CEO and highly recommended for other county government entities.

R.5. OCIT should develop a formal five-year cybersecurity strategic plan as a separate part of the IT Strategic Plan in the next county strategic plan.

R.6. OCIT should finalize a mandatory county incident response plan with procedures for individual agency exceptions and present it to the appropriate oversight bodies and BOS for approval by 7/1/2018.

R.7. The county should include in its 2018-19 IT Strategic Plan the identification, documentation and categorization by risk of county digital sensitive information.

R. 8. The county should annually review and update the amount and types of county cyber insurance based on the annual county risk analysis.

R.9. OCIT should implement cybersecurity training and professional certification of all county IT analysts having cybersecurity as a part of their job responsibilities by 7/1/2018.

R.10. OCIT should establish audit and test procedures to periodically, but no less than every two years, gauge the effectiveness of training and other cybersecurity measures by 7/1/2018.

R.11. The county should establish separate budget line items for cybersecurity expenses and capital investments for the 2018-2019 budget.

R.12. The county should implement the use of regional cooperative agreements for the acquisition of all cybersecurity related products and services by 7/1/2018.

R.13. The county should review and update IT job classifications and salary levels to reflect the current job market by 6/30/18.

R. 14. The county should develop a succession plan covering cybersecurity-critical positions by 6/30/18 to provide for continuity of these positions.

R. 15. Procedures for updating and patching all county software and systems that have been established by OCIT for the shared services program should be made mandatory for all county departments and agencies that report to the CEO, and recommended for all other county government entities by 6/30/18.

R 16. OCIT should draft and implement standardized procedures for mandatory use of full disk encryption and remote find/wipe capabilities for countywide mobile devices by 7/1/2018.

R. 17. OCIT should establish standardized procedures for IT's examination and removal of all sensitive information on county digital devices, prior to their removal from county premises through transfer, sale, scrap or reuse by 12/31/17.

R. 18. OCIT should establish standardized procedures for conducting periodic cybersecurity vulnerability and penetration testing by 12/31/19.

REQUIRED RESPONSES

The California Penal Code §933 requires the governing body of any public agency which the Grand Jury has reviewed, and about which it has issued a final report, to comment to the Presiding Judge of the Superior Court on the findings and recommendations pertaining to matters under the control of the governing body. Such comment shall be made no later than 90 days after the Grand Jury publishes its report (filed with the Clerk of the Court). Additionally, in the case of a report containing findings and recommendations pertaining to a department or agency headed by an elected County official (e.g. DA, Sheriff, etc.), such elected County official shall comment on the findings and recommendations pertaining to the matters under that elected official's control within 60 days to the Presiding Judge with an information copy sent to the Board of Supervisors.

Furthermore, California Penal Code Section §933.05 (a), (b), (c), details, as follows, the manner in which such comment(s) are to be made:

(a) As to each Grand Jury finding, the responding person or entity shall indicate one of the following:

(1) The respondent agrees with the finding

(2) The respondent disagrees wholly or partially with the finding, in which case the response shall specify the portion of the finding that is disputed and shall include an explanation of the reasons therefore.

(b) As to each Grand Jury recommendation, the responding person or entity shall report one of the following actions:

(1) The recommendation has been implemented, with a summary regarding the implemented action.

(2) The recommendation has not yet been implemented, but will be implemented in the future, with a time frame for implementation.

(3) The recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a time frame for the matter to be prepared for discussion by the officer or head of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This time frame shall not exceed six months from the date of publication of the Grand Jury report.

(4) The recommendation will not be implemented because it is not warranted or is not reasonable, with an explanation therefore.

(c) If a finding or recommendation of the Grand Jury addresses budgetary or personnel matters of a county agency or department headed by an elected officer, both the agency

> or department head and the Board of Supervisors shall respond if requested by the Grand Jury, but the response of the Board of Supervisors shall address only those budgetary /or personnel matters over which it has some decision making authority. The response of the elected agency or department head shall address all aspects of the findings or recommendations affecting his or her agency or department.

Comments to the Presiding Judge of the Superior Court in compliance with Penal Code section §933.05 are required from:

Responses Required:

Orange County Board of Supervisors (Findings F.1. – F.8.; Recommendations R.1 - 18.).

Responses Requested:

County Executive Office (Findings F.1. – F.8.; Recommendations R.1., R.3., R.7., R.8., R.11., R.12., R.13., R.14., R.15.).

Orange County Information Technology (Findings F.1. – F.8.; Recommendations R.2., R.4., R.5., R.6., R.9., R.10., R.15., R.16., R.17., R.18.).

REFERENCES

Akamai. (2016). *State of the Internet Security Q3 2016 Report.* Akamai.

Chuang, E. (2017). It's Not You, It's Your Vendor: The Hidden Doorway to Phishing Attacks. *Legaltech news*, p. 2. Retrieved 5 1, 2017, from http://www.legaltechnews.com/id=1202784938919/Its-Not-You-Its-Your-Vendor-The-Hidden-Doorway-to-Phishing-Attacks?kw=It%27s%20Not%20You%2C%20It%27s%20Your%20Vendor:%20The%20Hidden%20Doorway%20to%20Phishing%20Attacks&et=editorial&bu=Law%20Technology%20News&

Grimes, R. A. (2017). 9 new hacks coming to get you. *CSO Online*, p. 9. Retrieved 2 21, 2017, from http://www.csoonline.com/article/3171741/security/9-new-hacks-coming-to-get-you.html?idg_eid=c35b9224fe3bb5b632c1e442a73c4ba4&email_SHA1_lc=fa902d91c1aebeb660bfe968f17cf604cb88c00b&utm_source=Sailthru&utm_medium=email&utm_campaign=CSO%20Update%202017-02-2

ISO - ANSI. (2010). *The Financial Management of Cyber Risk.* New York: Internet Security Alliance (ISA)/American National Standards Institute (ANSI). Retrieved 2 21, 2017, from https://share.ansi.org/khdoc/Financial+Management+of+Cyber+Risk.pdf

Kaspersky. (2015). *The Threats From Within: How educating your employees on cybersecurity can protect your company.* Kaspersky Lab. Retrieved 2 17, 2017, from usa.kapersky.com

Masunga, S. (2017). Target settles with states over breach. *Los Angeles Times*. Retrieved May 24, 2017

Microsoft. (2016). *Intelligent Security: Using Machine Learning to Help Detect Advanced Cyber Attacks.* Microsoft Corporation. Retrieved 2 2, 2017, from https://www.microsoft.com/en-us/security/intelligence?&WT.srch=1&WT.mc_id=AID__SEM_Ta9wKfnh

National Association of Corporate Directors. (2017). *Cyber-Risk Oversight.* Washington, D.C., USA: National Association of corpoprate Directors. Retrieved 2 23, 2017, from https://www.nacdonline.org/cyber

NIST. (2012). *Computer Security Incident Handling Guide - Special Publication 800-61.* National Institute of Standards and Technology, Computer Security, Information Technology Laboratory. Gathersberg: National Institute of Standards and Technology. Retrieved 1 30, 2017, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST. (2013). *Glossary of Key Information Security Terms.* (R. Kisswel, Ed.) Retrieved 1 19, 2017, from National Institute of Standards and Technology: http://dx.doi.org/10.6028/NIST.IR.7298r2

NIST. (2016). *Small Business Information Security: The Fundamentals.* Gaithersburg: National Institute of Standards and Technology Applied Cybersecurity Division, Information Technology Laboratory. Retrieved 1 30, 2017, from https://doi.org/10.6028/NIST.IR.7621rl

Orange County Information Technology. (2017). *Implementing a Shared Services Strategy for Information Technology.* Santa Ana: OCIT. Retrieved 5 13, 2017, from http://cams.ocgov.com/Web_Publisher/Agenda01_24_2017_files/images/O00316-001666A.PDF

Phishlabs. (2017). *2017 Phishing Trends & Intelligence Report: Hacking the Human.* Charleston: ECrime Management Strategies, Inc. Retrieved 2 27, 2017, from https://pages.phishlabs.com/rs/130-BFB-942/images/2017%20PhishLabs%20Phishing%20and%20Threat%20Intelligence%20Report.pdf?mkt_tok=eyJpIjoiWkdVeFpESTRNek0xTm1GaCIsInQiOiJNdFhhR1pvcUVmbXdXaDhrMWE5KzVvV25qRDRodzFKdnlsK3NyeGVZWWNkYTN0SDErR2pWVG81YTJ1Tzdvc05zOH

Plante Moran. (2014). *Enterprise Resource System Security Audit Report (Phase 3.0, 4.0 and 5.0 Combined).* Cerritos: Plante Moran.

Ponemon Institute. (2016). *2016 Cost of Data Breach Study.* Ponemon Institute.

Privacy Rights Clearinghouse. (2017). *Chronology of Data Breaches.* Retrieved from Privacy Rights Clearninghouse: https://www.privacyrights.org/data-breaches

PwC. (2016). *Key findings from the Global State of Information Security 2017.* PwC. Retrieved 2 17, 2017, from http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf

SANS Institute. (2017). *Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017.* Bethesda: SANS Institute. Retrieved May 12, 2017, from https://www.sans.org/reading-room/whitepapers/analyst/cyber-security-trends-aiming-target-increase-security-2017-37702

Straight, J. (2017). *5 Key Cyber Trends Dominating the Early 2017 Discourse.* Retrieved 3 6, 2017, from Legaltech News: http://www.legaltechnews.com/id=1202780585472/5-Key-Cyber-Trends-Dominating-the-Early-2017-Discourse?kw=5%20Key%20Cyber%20Trends%20Dominating%20the%20Early%2020

17%20Discourse&et=editorial&bu=Law%20Technology%20News&cn=20170306&src=EMC-Email&pt=Daily%20Ale

Symantec. (2016). *Internet Security Threat Report.* Symantec. Retrieved 1 20, 2017

U.S. Department of Justice. (2015). *Best Practices for Victim Response and Reporting of Cyber Incidents.* Cybersecurity Unit, Computer Crime and Intellectual Property Section, Criminal Division. U.S. Department of Justice. Retrieved 1 30, 2017, from https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf

Verizon. (2016). *2016 Data Breach Investigations Report.* Verizon.

APPENDICES

Appendix A: Sources of Cybersecurity Standards and Best Practices

AICPA (American Institute of CPAs) Cybersecurity Resource Center - http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/cybersecurity-resource-center.aspx

BugTraq by SecurityFocus (Symantec) - http://www.securityfocus.com/

Cal OES (The California Cybersecurity Task Force) - http://www.caloes.ca.gov/for-individuals-families/cybersecurity-task-force)

CIS (Center for Internet Security) - https://www.cisecurity.org/

CSIS (Center for Strategic & International Studies, Cyber Task Force) - https://www.csis.org/programs/strategic-technologies-program/cybersecurity/csis-cyberpolicy-task-force

Department of Justice, Cybersecurity Unit – http://www.justice.gov

FCC (Federal Communication Commission, Planning Guide) - https://transition.fcc.gov/cyber/cyberplanner.pdf

The Federal Risk and Authorization Management Program (FedRamp) - https://www.gsa.gov/portal/category/102371

FINRA (Financial Industry Regulatory Authority) - www.finra.org/

FTC (Federal Trade Commission) - https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

FBI (Federal Bureau of Investigation) - https://www.fbi.gov/investigate/cyber)

GSA Cybersecurity Site - https://www.gsa.gov/portal/category/101078

HIPAA (Health Insurance Portability and Accountability Act) - https://www.hhs.gov/hipaa/

HITECH (The Health Information Technology for Economic and Clinical Health Act) - https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

ISACA (Information Systems Audit and Control Association) - https://www.isaca.org/pages/default.aspx

ISO/IEC 27032 Cybersecurity Standards - http://www.iso27001security.com/html/27032.html

ISO/IEC 27001 Information security management - http://www.iso27001security.com/html/27001.html

MS-ISAC (Multi-State Information Sharing Analysis Center) - https://msisac.cisecurity.org/

NASCIO (National Association of State Chief Information Officers) - https://www.nascio.org/

National Council of ISAC's - http://www.isaccouncil.org/

The National Cyber Security Alliance (NCSA) - https://staysafeonline.org

NCCIC (Homeland Security National Cybersecurity & Communications Integration Center) - https://www.us-cert.gov/nccic

NHTSA (National Highway Traffic Safety Administration) - https://www.nhtsa.gov/

National Institute of Standards and Technology (NIST)
Standards - https://www.nist.gov/cyberframework
US National Vulnerability Database – https://nvd.nist.gov

NSTIC (National Strategy for Trusted Identities in Cyberspace - https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

OCIAC (Orange County Intelligence Assessment Center) - https://ociac.ca.gov/

Orange County Cybersecurity Program - http://www.ocgov.com/gov/ceo/cio/initiatives/security

OCRCFL (Orange County Regional Computer Forensics Lab) - https://www.rcfl.gov/orange-county

PRC (Privacy Rights Clearinghouse) - https://www.privacyrights.org/data-breaches)

Presidential Executive Order 13636 (Improving Critical Infrastructure Cybersecurity (EO 13636); https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

SCHTTF (Southern California High Tech Task Force - https://oag.ca.gov/ecrime/httap)

Security Intelligence Web Site - https://securityintelligence.com/

UL Labs Cybersecurity Site (http://www.ul.com/cybersecurity/)

US-CERT (United States Computer Emergency Readiness Team) - https://www.us-cert.gov/
U.S. Department of Homeland Security Cyber Security Resources – http://www.dhs.gov/cyber

U.S. Department of Homeland Security (National Cybersecurity (FFDRC) Common Vulnerabilities Exposures System Lists) - https://www.mitre.org/centers/national-cybersecurity-ffrdc/who-we-are

Appendix B: Types of Cyber Attacks

Denial of service (DoS). This type of attack involves overwhelming the web site or device with so many incoming requests that it results in prevention of authorized access to resources or delay of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided (NIST, 2013)). This can result in the unavailability of needed services or devices for a period of time, with a resulting negative impact on productivity and responsiveness. Denial of Service attacks increased 71% increase from 2015 to 2016 (Akamai, 2016).

Compromise of the Internet of Things (IoT). The IoT is the worldwide grouping of smart devices all connected via the internet and capable of sending and receiving data. These devices include PCs, servers, routers, switches, smart phones, tablets, Internet phones, smart light bulbs, web cameras, cloud-connected data storage devices, DVD's, home routers, smart TVs and connected home/home security equipment as well as printer/copiers, cars, industrial control systems such as utility providers, HVAC and building management systems, medical devices such as pacemakers, heart monitors, IV drip devices, diagnostic machinery and even web connected toys (Grimes, 2017). Manufacturers are increasingly connecting their devices to the internet with the ability to stream (send) data out but many lack the ability to be patched or managed (Akamai, 2016, p. 29).

Social Engineering. A general term for human error, device loss, theft, or unintended disclosure. Generally this involves attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious (NIST, 2013). Human beings are generally recognized as the weakest link in the cybersecurity chain in any organization and, according to a 2015 survey by Kaspersky Labs, 42% of confidential data loss is due to organization employees (Kaspersky, 2015). The end result is that no matter how much is spent on state of the art cybersecurity software, your data is just one gullible click away from compromise.

Phishing, a type of social engineering, is an email or electronic communications scam targeted towards a specific individual, organization or business. The email may offer a prize, access to a fortune in another country or appear to be from a company executive directing a transfer of funds. Phishing is the top vector identified in 2016 for cyber attacks (Phishlabs, 2017). According to a recent survey, in 2016, 38% of respondents reported phishing incidents (PwC, 2016). The volume of phishing attacks on government entities increased by 80% in 2016, primarily due to attacks on tax entities, particularly the IRS (Phishlabs, 2017). There are several variations of Phishing:

Spear-phishing, focused on a specific individual or group;
Whale phishing, focused on a senior executive;
Business email compromise occurs when executive email accounts are used to direct a company employee to transfer money to a fictitious supplier. In January of 2015, the FBI indicated that thieves had stolen nearly $215 million in the previous 14 months using this type of scam.
Ransomware, the most common type of phishing (Phishlabs, 2017), targets end users and the networks they have access to, uses malware to encrypt the user's files (and files

of other computers on any network connected to that user's computer), allowing the cybercriminals to demand a ransom in exchange for the key to unlock the encrypted files. Ransomware incidents increased 35% in 2015 (Symantec, 2016) and, in addition to PCs, smart phones, communication systems, smart watches and even televisions have been found to be vulnerable (Symantec, 2016). Indicators of a phishing email include:

- Spelling or grammatical mistakes.
- An unfamiliar sender, sent-from address, or URL.
- The sent-from name does not match the sender.
- A request to transfer money.
- The sender asks for personal information.
- What is offered seems too good to be true or unreasonable.
- The language in the email is urgent or threatening.

Vendor as a vector. Most organizations have business relationships with a number of outside partners and vendors, many of whom are now digitally connected to the organization's IT systems and data. These relationships need to be assessed and managed in the area of cybersecurity. This is when the intruding malicious actor penetrates a vendor that has legitimate access to another organization's data (point of sale system vendors, database services, etc.) and uses the vendor-partner's legitimate credentials to gain access to the organizations data. Organizations should consider the impact of potential key vendors cyber breaches and ensure that vendor contracts contain clauses mandating vendor cybersecurity, include service level guarantees for cybersecurity and provisions for audit of the vendor's cybersecurity systems and status.

Penetration Hacking/Intrusion is the unauthorized bypassing of a system's security mechanisms. This is generally accomplished through the use of malware, which are computer programs written especially to penetrate network and operating system defenses. One example of this is a zero-day vulnerability (see below). This highlights the necessity of updating and patching the software being used by an enterprise on a timely and complete basis to avoid these attacks.

Website Compromise, also known as **water holing**, is the use of hidden or deceptive programming on a website to capture data about the user visiting the website or insert malicious programming onto the user's computer and/or network. A user clicking on "allow" or "confirm" in a drop down menu can execute the malicious code and can infect the users system (Kaspersky, 2015). There were over one million web attacks against users daily in 2015. Over 75% of legitimate websites have unpatched vulnerabilities and 15% of those are deemed critical (Symantec, 2016), meaning that it takes little effort for hackers to gain access and use these websites for their own purposes.

Zero-Day Infections/Attacks are unknown or undisclosed security vulnerabilities in computer software or applications for which either the patch has not been released or the application developers were unaware of or did not have sufficient time to address, leaving the software's author with zero days in which to create patches or advise workarounds to mitigate its actions. In 2015, the number of new zero day vulnerabilities more than doubled, from 54 in 2014 to 154, up from 23 in 2013. (Symantec, 2016). One disturbing trend is the commercialization of exploit

kits on the black market, making it easier for hackers to quickly take advantage of vulnerability. (Symantec, 2016)

Appendix C: Orange County Information Technology Oversight Bodies

The IT Executive Council consists of the county chief information officer, chief financial officer, chief human resources officer, one elected department head, two IT customer department heads from the shared services pilot program; it is chaired by the county CEO. This group meets quarterly and is responsible for reviewing and approving IT policy, IT strategic plans, annual IT project funding recommendations and IT operating and performance metrics.

The Technology Council meets bimonthly and provides technical guidance and recommendations to the IT Executive Council regarding IT initiatives, policies and investments.

The IT Shared Services Steering Committee provides executive leadership for the implementation of an IT service strategy enabling county agencies and departments to access central contracts.

The IT Investment Review Committee evaluates, prioritizes and makes recommendations to the IT Executive Council regarding IT project proposals and associated funding requests.

The Cyber Security Joint Task Force pursues several important cybersecurity initiatives expected to be implemented in 2017. Consisting of representatives from county counsel, risk management, department administrative services and information technology, and chaired by the county CISO, the group is developing cybersecurity policies and procedures with common standards for all county departments.

The Audit Oversight Committee, which oversees all county audit functions and consists of representatives from the offices of the Auditor-Controller, Treasurer, CEO, all appointed and elected agency heads, County Counsel and the CISO.