# Building a Municipal Comprehensive Next Generation Cyber Security Program – Riverside, CA

#### **Problem Assessment**

Cyber security programs across the nation are struggling to contain a growing threat to our nation's critical infrastructure. The majority of organizations approach cyber security threats solely as a technology problem or focus on a single problem. Unfortunately, attackers are targeting both technology and people. Legacy cyber security programs focus solely on technology missing the human attack surface and resulting in significant security breaches.

Malicious cyber actors have been leveraging the same tactics for decades. For example, in December 1994 Kevin Mitnick launched an attack against an employee's home computer to exploit its trusted remote access connection to Motorola's secure network resulting in a breach of Motorola's cellular source code. Fast forward twenty-three years and attackers are still targeting trusted access channels to bypass security controls.

Another example occurred in 2013 when Target suffered a major breach resulting in the theft of more than 40 million credit cards. The attack was initiated by targeting someone with an established trusted access. Target's external HVAC contractor was compromised allowing the attackers to bypass Target's hardened external security and provided the attacker with access to internal systems including point of sale systems. Target's board did not anticipate nor prepare for this attack because as they put it, "they sell socks."

The Ukraine suffered a massive power outage affecting more than 225,000 customers in December 2015. It was quickly determined that the attack was initiated by exploiting employees using a spear-phishing email with an attached spreadsheet containing what appeared to be a national military personal activation list. The attachment turned out to be a "weaponized" document allowing attackers access to the Ukraine power system.

These attacks highlight that a successful security program must not only secure technology but also change people's behavior to be successful. Technology alone failed to protect the organizations identified above from a persistent and skillful attacker.

The City of Riverside is the 12<sup>th</sup> most populous City in California providing world class service to 305,000 residents. The City operates multiple critical infrastructure services such as public safety, power and water resources, wastewater services, community and economic development and library and community enrichment programs. In 2015, the City of Riverside recognized cyber security risks and created a cyber security division to lead citywide cyber security efforts. The division was tasked with identifying areas of risk in technology, business processes, and employee behavior. The division was tasked with creating, implementing and enforcing a comprehensive and forward-looking security program.

#### **Program Implementation and Costs**

Riverside's security program's vision seeks to leverage, develop and even extend the capabilities of commercial and open source products to protect the City's critical systems and users. The program acknowledges and embraces the fact that the security of an organization is reduced to the weakest link in technology, business process, internal user or 3<sup>rd</sup> party partner. The City of Riverside's comprehensive security program extends beyond technology and reaches within the Citywide business operations cyber risk management as well as employee training and assessment. The City of Riverside is leading regional cyber security outreach extends information sharing to sister cities, organizations as well as the Riverside business community. The City introduced the residents to cyber security awareness month in October 2016 through a cyber security public service announcement, council declaration, and billboards. Riverside presented cyber risk to the chamber of commerce members and hosted a regional cyber security symposium in 2016.

The Cybersecurity division implemented the following defense in depth programs included the following at a total cost of \$24,517:

- Advanced Next Generation Firewall protections:
  - The cyber security division was formed in the midst of an existing firewall upgrade project. The initial scope of the upgrade was extended to combat advanced threats by leveraging or extending the capability of existing platforms to reduce cost.
  - The firewall's antivirus capabilities were extended beyond manufacturer default deployment recommendations to block unauthorized file downloads. Next generation "zero-day" or unknown malware protection features were implemented to analyze all inbound files and emails in a virtual sandbox. Email attachments sanitization was deployed to prevent email focused Ukraine-style attacks. Advanced intrusion prevention protections, anti-bot, and user content filtering were also deployed.
  - Traffic analysis was performed and identified that internet traffic is increasingly encrypted. Nearly 40 percent of all City internet traffic was transmitted using Secure Socket Layer "SSL". Legacy firewalls as well as typical deployments of next generation firewalls fail to prevent or detect attacks within encrypted communications. As a consequence, attackers are leveraging SSL encryption to bypass most security controls. Riverside's security division implemented SSL inspection to provide equal protection to encrypted and non-encrypted traffic. SSL inspection is a significant accomplishment due to the complexity and required technical expertise to implement and maintain the inspection protection.

#### • Integrating Cybersecurity within Citywide Business processes:

 Cyber Security Governance Committee - A comprehensive cyber security program requires transparency, accountability, and openness to embrace change. Riverside's Cyber Security Governance Committee is composed of department heads or their deputies and provides monthly security progress updates on upcoming initiatives. The committee provides a platform to make informed business decisions and increase the City's security posture through security controls, business process changes, and employee awareness while keeping business needs and customer service at the forefront. The cost of this program is limited to staff time.

 Data Loss prevention project - Prevention is ideal, but risk management is the cornerstone of comprehensive security program. The vast majority of attackers exploit people and technology to gain access to information. A persistent attacker with sufficient resources and talent will penetrate most defenses. A mature security program will build solid defenses but recognizes that intrusions are becoming a fact of life. Federal, military and private sector breaches are a daily headline. Riverside's security approach leverages next generation defensive measures and seeks to reduce liability and exposure.

The Security division launched a data loss prevention pilot project In 2016. The project's goal was to identify the proliferation of sensitive data across the organization, which business processes are generating protected data and most importantly change processes to reduce risk. The project is a forward-thinking hybrid security initiative of technology, business, and employee awareness. The project identified several million non-unique sensitive records scattered across the organization. The cost of the pilot was under \$2,500.

Since technology alone can not solve business process gaps, the City formed a cross-functional data loss prevention task force to review, remediate and modify risky business processes. Each department reviewed and remediated their findings according to the City's legal and records retention policies. The majority of the findings identified duplicate data or records that have exceeded their retention schedule. Changing risky business processes was an important outcome of this project. Departments are now fully aware of the data contained in their reports. Sensitive records are now being obfuscated or is being sent using protected channels and destroyed when no longer needed significantly reducing the City's exposure and liability if a cyber event occurs.

Employee awareness - Users are the source of over 70 percent of the recent cyber breaches. Riverside's security program utilizes a "train, assess and remediate framework." The City exposes new employees to cyber security risks as a part of their orientation. The City also deployed an annual mandatory cyber security awareness training program. Employees must complete a customized business specific security awareness program. Each program is carefully crafted to address risk exposure within each business unit and addresses any applicable regulatory or compliance requirements. Employees complete brief multiple choice questions after each module to encourage retention of the training material. Employees lose access to the City network if they fail to

complete the training by the established deadline. The training system costs the City approximately \$6,000 per year.

The City conducts Cyber training assessment by launching simulated phishing campaigns to identify high-risk employees. Employees that fail the simulation are required to retake the security awareness training, and their department head is notified. The City is exploring adding cyber security score to the employee's annual performance reviews as a reinforcement that cybersecurity is a shared responsibility among all employees. The City abandoned commercial phishing simulation software due to the high cost. Vendor estimates ranged between \$15,000 – \$33,000 per year. The City's security division deployed an open source solution in Amazon AWS at the cost of \$17 per simulated exercise. The City also deployed a free "Phish-Alert" button to all outlook installations putting the awareness and threat of phishing attacks at the forefront of employees email client. Employees are actively utilizing the tool to report phishing emails.

Information Sharing and community outreach - The City's security division is a strong advocate of cyber security within the community. The City has reached out to the community to raise awareness, reduce fraud and reduce the number of incidents such as ransomware and social engineering that impact local businesses. Outreach efforts include local speaking engagements, community public service announcements, council declarations supporting the national cyber security awareness "stop, think, connect" campaign, and local business outreach through the various Chamber of Commerce entities. The City also hosts an annual regional cyber security symposium to share security best practices with regional entities. The City formed a cybersecurity leadership group that meets quarterly with local cities, water districts and local businesses to share intelligence, success, and failures as well as improve security across the organizations by sharing best of breed strategies. The program costs are limited to staff time.

**3**<sup>rd</sup> **party risk management -** Riverside's security division is reviewing and auditing new vendors to ensure compliance with its security standards and best practices. The City is updating security policies along with cyber security insurance policies to improve the City's risk management posture and reduce the likelihood of a third party incident.

## Tangible Results or Measurable Outcomes of the Program

Cyber security is now an integral part of all new project. Security awareness succeeded in making employees more risk aware and has led to may "stop and think" moments. City employee awareness of cyber risk is at an all-time high with employees proactively alerting their teams and IT if they suspect phishing. Outcome examples include:

• Ransomware infections have been virtually eliminated with no reported incidents in the past 12 months. Previously the City experienced a

ransomware attack quite regularly. Internet-sourced virus infections have been reduced from 3-5 daily events to less than one event monthly.

• The City also eliminated a large number of protected records via the data loss prevention effort. Using Forbes' estimate of a \$214 cost per record breached, the City removed potential liability of nearly one billion dollars had someone breached the City's unique and sensitive data.

## Lessons Learned During Planning, Implementation, and Analysis of the Program

Cyber security programs typically fail because of lack of a comprehensive vision, lack of business acceptance or simply failing to acknowledge business needs. Riverside's cybersecurity comprehensive plan addresses a large number of phases of the attack lifecycle. Riverside implemented defense in depth leveraging technology, risk management, employee training and engagement as well as business process rearchitecture.

Implementing the Riverside's security program required leadership support with deep technical, business and customer service understanding. Partnering with the organization is crucial to adoption, success and the ultimate goal to change behavior. By utilizing user engagement, data remediation ownership, as well as business process re-architecture, the project developed a healthy level of risk awareness with leadership and departments that will benefit the City for years to come.

Management and user acceptance of cyber security risk is crucial as a more secure process does not always mean a simple or easy change and could result in business process realignment. The data loss prevention findings, employee security awareness training and phishing simulation results were praised by the management team. The project involved employees with data cleanup as well as engaging them with phishing simulation results resulted with employees identifying previously unknown risks and recommending more secure processes.

Security budget could be a challenge even when risk is clearly understood. The City fully funded the next generation firewall and the security awareness training however the data loss prevention and the phishing simulation were unfunded projects. To overcome lack of funding, the City implement data loss prevention as a limited proof of concept pilot at a likely high-risk area and was a huge success. The phishing simulation used an open source product also resulting in a successful effort. Due to these successes, the City will identify future funding to expand the security tools and efforts.

# How the Program Raises Awareness of the Contributions of Local Government Managers

Security's ultimate goal is to change behavior. The change should start with system owners and technical staff to make day to day operations more secure and extended to all users when they pursue new products or access the web or their email. Local government managers are dependent on technology to provide services to the public. Attackers are exploiting this dependency to disrupt public service operations and exploit organizations. Riverside's comprehensive cyber security program emphasizes increasing security to allow local managers to perform their core business functions and provide world class customer service to our citizens.