COUNTY OF MADERA
BUDGET UNIT DETAIL
BUDGET FOR THE FISCAL YEAR 2024-25

Department:	**Information Technology Security (00243)**
Function:	**General**
Activity:	**Other General**
Fund:	**General**

	ACTUAL 2022-23	BOARD APPROVED 2023-24	DEPARTMENT REQUEST 2024-25	CAO RECOMMENDED 2024-25
ESTIMATED REVENUES:				
INTERGOVERNMENTAL REVENUE				
CHARGES FOR CURRENT SERVICES				
662800 Interfund Revenue	0	49,623	40,949	40,949
662802 Interfund Rev - Comp Svc	49,623	0	0	0
TOTAL CHARGES FOR CURRENT SERVICES	**49,623**	**49,623**	**40,949**	**40,949**
MISCELLANEOUS REVENUE				
670000 Intrafund Revenue	1,884,382	2,698,966	3,200,690	3,200,690
TOTAL MISCELLANEOUS REVENUE	**1,884,382**	**2,698,966**	**3,200,690**	**3,200,690**
TOTAL ESTIMATED REVENUES	**1,934,005**	**2,748,589**	**3,241,639**	**3,241,639**
EXPENDITURES:				
SALARIES & EMPLOYEE BENEFITS				
710102 Permanent Salaries	371,767	595,898	760,246	760,246
710105 Overtime	6,230	3,000	3,000	3,000
710106 Stand-By	24,316	26,624	26,624	26,624
710200 Retirement	147,524	241,994	321,052	321,052
710300 Health Insurance	30,252	121,710	121,736	121,736
710400 Workers' Compensation Insurance	0			
TOTAL SALARIES & EMPLOYEE BENEFITS	**580,089**	**989,226**	**1,232,658**	**1,232,658**
SERVICES & SUPPLIES				
720300 Communications	3,438	4,500	6,000	6,000
720800 Maintenance - Equipment	81,683	77,500	142,349	142,349
721300 Office Expense	36,910	19,000	10,000	10,000
721307 Computer Equipment <$5,000	0	16,000	5,000	5,000
721400 Professional & Specialized Services	382,058	651,395	626,246	626,246
721426 Software	832,419	815,995	1,153,966	1,153,966
721500 Advertising	0	0	2,000	2,000
721900 Special Department Expense	3,319	18,000	15,000	15,000

COUNTY OF MADERA
BUDGET UNIT DETAIL
BUDGET FOR THE FISCAL YEAR 2024-25

Department:	**Information Technology Security (00243)**
Function:	**General**
Activity:	**Other General**
Fund:	**General**

	ACTUAL 2022-23	BOARD APPROVED 2023-24	DEPARTMENT REQUEST 2024-25	CAO RECOMMENDED 2024-25
SERVICES & SUPPLIES (continued)				
722000 Transportation & Travel	26,910	37,380	51,190	51,190
TOTAL SERVICES & SUPPLIES	**1,366,736**	**1,639,770**	**2,011,751**	**2,011,751**
OTHER CHARGES				
730330 Rent	337,756	415,740	335,596	335,596
TOTAL OTHER CHARGES	**337,756**	**415,740**	**335,596**	**335,596**
FIXED ASSETS				
740300 Equipment	0	145,000	104,101	104,101
TOTAL FIXED ASSETS	**0**	**145,000**	**104,101**	**104,101**
TOTAL EXPENDITURES	**2,284,581**	**3,189,736**	**3,684,106**	**3,684,106**
NET COUNTY COST (EXP - REV)	**350,576**	**441,147**	**442,467**	**442,467**

COMMENTS

In alignment with the organizational strategic initiatives established by the Executive Technology Steering Committee, the Office of Information Technology (OoIT) will continue advancing its Information Security Strategy into Fiscal Year 2024-2025. This year marks a new phase following the significant improvements in compliance and security posture achieved during the previous strategic period. The enhancement in posture is attributed to the ongoing optimization of tools, making this a primary focus for Fiscal Year 2024-2025. As adversaries evolve, compliance requirements tighten, and insurance demands escalate, there is a pressing need to deploy new technology and processes. In this fiscal year, OoIT will further enhance our security layers to counteract new threats and address protection gaps. A sustained focus will be placed on the human element, with expanded efforts in phishing simulation and security awareness training. Efforts will also be directed towards reducing risk by increasing our edge defense, email protection via AI, and continued focus on disaster recovery. The objectives of the information security program remain to safeguard the confidentiality of information, maintain the integrity of data, and increase the availability of systems and operations. By leveraging compliance and insurance requirements as a framework, the information security program aims to fortify the security surrounding Federal Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Criminal Justice Information Services (CJIS), Federal Tax Information (FTI – Publication 1075), and other privacy mandates, thereby enhancing the confidentiality, integrity, and availability of the County’s networks, systems, and data.

The following chart represents Madera County Departments that have been identified as receiving and/or exchanging Federal information.

Sheriff's Department	Department of Justice
Department of Corrections	Department of Justice
Probation	Department of Justice
District Attorney	Department of Justice, Department of Treasury
Child Support Services	Department of Treasury, Social Security Administration
Department of Social Services	Department of Treasury, Social Security Administration, Department of Justice
Public Health	Social Security Administration and Women, Infants and Children
Behavioral Health Services	Social Security Administration

The "Verizon 2023 Data Breach Investigations Report" highlights several critical trends in cybercrime that public sector agencies, including the County of Madera, should be aware of. The report shows a significant increase in the cost and frequency of social engineering attacks, with ransomware incidents becoming particularly expensive. Ransomware now constitutes nearly a quarter of all data breaches. Additionally, the human element continues to be a major factor in breaches, being involved in about three out of every four incidents. This includes various forms of social engineering attacks, as well as errors and misuse. Notably, Business Email Compromise (BEC) attacks and pretexting incidents have seen a substantial rise, with pretexting incidents nearly doubling compared to the previous year. This underscores

COMMENTS (continued)

the need for public sector entities to strengthen their cybersecurity measures, focusing not only on technological solutions but also on training and awareness programs to address the human aspect of security. It also highlights the importance of robust incident response plans and the investment in adequate resources, including staffing and partnerships, to counter these evolving threats. The County is focusing on conducting real-world phishing simulations and providing specific training on phishing. This is particularly relevant considering the report's indication that 50% of all social engineering attacks are now pretexting incidents, nearly double compared to the previous year.

In addition to strengthening the human element, OoIT is also integrating specific technologies that are essential in modern cybersecurity defense. These include advancing intrusion detection systems (IDS) for monitoring network traffic for suspicious activity, upgrading and enhancing next-generation firewalls (NGFWs) that go beyond traditional firewall capabilities to provide more granular security controls, and endpoint detection and response (EDR) solutions for continuous monitoring and response to advanced threats. Additionally, reviewing and enhancing our audit logging integrate into information and event management (SIEM) systems will enable comprehensive analysis of security alerts generated by applications and network hardware. This multifaceted approach, combining skilled personnel, specific training, and advanced technology, positions the County to effectively counter the evolving landscape of cybersecurity threats.

WORKLOAD

Key components of the Information Security budget include:

- Development, upkeep, and success measurement of Information Security Program; including but not limited to, security governance, strategy, policies, standards, control implementation, contract hardening, etc.
- Threat, Vulnerability, Impact Assessment, and Patch Management
- Identity and Access Management
- Backup management – policy, retention development, auditing (report monitoring), validate recovery testing.
- Inventory and System Development Life Cycle (SDLC)
- Network Monitoring Operations & Security Monitoring Operations
- Incident Management
- Security Awareness Training
- Data room physical security and data protection
- Threat Intelligence - Network threat detection and defense system management
- Security architecture, design, and control implementation
- Risk Assessment
- Technical Contract and Statement of Work Analysis

Security Division Accomplishments 2023-2024

- **Backup Data Protection from Ransomware:** The successful implementation of the Backup Data Protection project has significantly fortified our organization's resilience against ransomware attacks. This accomplishment is particularly noteworthy given the increasing prevalence and sophistication of such cyber threats. By deploying cutting-edge backup and recovery solutions, we have established a robust and multi-layered defense strategy. Our approach involved creating immutable backup copies, which are impervious to ransomware alterations, thus increasing the integrity and availability of our critical data. Moreover, we integrated advanced encryption methods to secure our backups, both in transit and at rest, further safeguarding them from unauthorized access. This proactive stance significantly enhances our cyber resilience, providing a vital safety net that minimizes the potential impact of ransomware incidents on our operations and reputation.
- **Legacy Protocol/Configuration/Features Vulnerability Remediation:** The "Legacy Protocol/Configuration/Features Vulnerability Remediation" project represents a pivotal accomplishment in enhancing our network's cybersecurity. This project successfully tackled the challenge of addressing three critical vulnerabilities found in our legacy protocols/configurations/features. These older configurations had become susceptible to various security risks. Our dedicated team conducted a thorough analysis to identify these specific vulnerabilities, implementing strategic solutions to effectively remediate them. The process involved replacing outdated configurations with advanced, more secure technologies, thereby not only resolving the immediate security concerns but also aligning our network infrastructure with contemporary cybersecurity standards. In other instances, the configuration was completely removed. This proactive approach to identifying and mitigating potential weaknesses in our legacy systems has significantly strengthened our defense against cyber threats, showcasing our unwavering commitment to maintaining robust and resilient cybersecurity defenses. Although major strides have been made in FY 23/24, this will be an ongoing initiative in the years to come as security is an ever-evolving journey and a destination is not the goal.
- **Browser Security Pilot:** This initiative focused on strengthening web browsing security, a crucial area in light of emerging online threats. The pilot effectively demonstrated the value of advanced browser security tools in protecting against risks such as phishing, malware, cached credentials, and nefarious browser plug-ins. Building on this success, the next phase involves a comprehensive rollout, intricately linked with an enterprise password management system.
- **Continued Optimization of Network Visibility Tools:** Our team has made significant progress in enhancing our security posture through the optimization of network monitoring tools. By improving visibility into our IT environment, we can now increase the detection of critical threats such as ransomware, internal unauthorized movement, unauthorized network scanning, fileless malware, abnormal network traffic, foreign traffic destinations (e.g. China, Russia, etc.), unauthorized script execution, data hoarding, and malware propagation. This achievement significantly improves the security posture of our organization in several ways. First, it allows us to identify and respond quickly to potential security incidents, minimizing the likelihood and impact of attacks, and reducing the risk of data loss or service disruptions. Additionally, this enables us to proactively address vulnerabilities and mitigate risk.

Security Division Accomplishments 2023-2024 (continued)

- **Microsoft 365 Data Backup:** This comprehensive solution has significantly enhanced our capability to securely backup and restore critical data hosted in the Microsoft 365 cloud environment. By implementing this system, we've increased robust protection against data loss scenarios, such as accidental deletions, system crashes, and potential security breaches. The M365 Cloud Backup Solution not only offers an added layer of security but also provides greater flexibility and control in data recovery, striving towards business continuity and compliance with data retention policies. Its successful integration into our IT infrastructure demonstrates our commitment to leveraging advanced technology solutions to safeguard our digital assets and maintain operational efficiency in an increasingly cloud-centric business landscape.
- **Disaster Recover Site Replication**: This initiative focuses on transporting our backup data to a secondary, remote site, thereby creating an additional layer of protection and redundancy. In the event of a backup data failure in our primary datacenter due to issues such as natural disasters, system failures, or cyber-attacks, this secondary site provides a reliable fallback for data recovery. This strategic approach not only bolsters our disaster recovery capabilities but also underscores our commitment to robust data management practices, ensuring operational resilience and continuity in a variety of challenging scenarios.

Anticipated Projects 2024-2025

- **Zero Trust Framework Advancement**
  - Increased Multi-Factor Authentication
  - Network Segmentation
  - Security Information and Event Management (SIEM) Strategy
  - Network Visibility Optimization

  Costs for this initiative are budgeted in Account 721314.

- **Health and Human Services Vulnerability Evolution**
- **Countywide Password Manager:** The "Countywide Password Manager" project is an initiative designed to enhance cybersecurity across all county departments by implementing a comprehensive password management solution. This project aims to streamline password management, reduce the risk of password-related breaches, and improve overall security practices by providing a secure, centralized system for storing and managing passwords. By equipping employees with a user-friendly password manager, the project seeks to encourage stronger password habits, eliminate the use of weak or repeated passwords, and increase efficiency in password

Anticipated Projects 2024-2025 (continued)

administration, contributing significantly to the county's cybersecurity posture and compliance with best practices. Costs for this initiative are budgeted in Account 721426.

- **Disaster Recovery (DR) Roadmap and Advancement**
    - Active Directory DR Planning
- **Secure Email Domain Record Advancement:** The DMARC/DKIM/SPF Implementation project is an initiative focused on strengthening email security across the organization by deploying three key email authentication protocols: Domain-based Message Authentication, Reporting, and Conformance (DMARC), DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF). This project aims to significantly reduce the risk of email phishing and spoofing attacks, enhancing the integrity and reliability of email communications. Costs for this initiative are budgeted in Account 721426.
- **Security Tool Alert/Threat Defense Optimization**
- **Malware Sandbox Safe Inspection & Analytics:** Implement an advanced malware analysis tool, allowing staff to quickly identify security threats in files. The tool looks at files for malicious code to determine its behavior and potential impact. This is done though threat intelligence, comparing suspicious files to know malicious code in a sandbox environment. The sandbox allows IT staff to run malware in a safe isolated environment to examine and analyze the code without exposing the organization to harm. Costs for this initiative are budgeted in Account 721426.
- **Replacement of Three (3) End of Life (EOL) Firewalls:** The existing firewall infrastructure located at the Coroner's Office, the County Clerk-Recorder's Office, and the Tesoro Viejo Fire Station will each reach the end of its operational life which can pose significant risks to the security and integrity of critical data and communication channels if not replaced. The firewall replacement is essential to fortify our network security and ensure the continued protection of sensitive information. Costs for this initiative are budgeted in Accounts 721426 and 740301.
- **Data Loss Prevention (DLP) Planning & Analysis Pilot Program:** The "DLP Pilot Project" is a focused initiative aimed at implementing data classification and Data Loss Prevention (DLP) strategies within a pilot department of a specific subdivision. This project serves as a testbed for evaluating the effectiveness of DLP tools and protocols in protecting sensitive information from unauthorized access or breaches. By piloting these measures in a controlled environment, the project aims to assess the feasibility, operational impact, and potential benefits of DLP solutions before a wider organizational roll-out. Costs for this initiative are budgeted in Account 721400.
- **Legacy Protocol/Configuration/Features Vulnerability Remediation:** Although major strides have been made in FY 23/24, this will be an ongoing initiative in the years to come as security is an ever-evolving journey and a destination is not the goal.

Unfunded Project 2024-2025

Due to budget limitations and the higher level of risk associated with competing projects, the Web Browsing History Reporting project will not be completed in Fiscal Year 2024-2025.

- **Web Browsing History Reporting:** The Web Browsing History Reporting project is designed to implement a comprehensive system for monitoring and reporting web browsing activities within the organization. This initiative aims to enhance oversight of internet usage as well as to identify potential cybersecurity threats. By tracking and analyzing web browsing patterns, the project will provide valuable insights into employee internet usage, enabling the organization to reinforce security protocols, optimize network resources, and mitigate risks associated with non-compliant or unsafe web activities.

ESTIMATED REVENUES

662802 **Interfund Revenue** ($40,949) is recommended decreased $8,674 for charges to other departments for Network Information Security Services.

670000 **Intrafund Revenue** ($3,200,690) is recommended increased $501,724 for charges to other departments for Network Information Security Services.

SALARIES & EMPLOYEE BENEFITS

Eight (8) funded positions is recommended unchanged.

710102 **Permanent Salaries** ($760,246) are recommended increased $164,348 to fund the current and new security positions.

710105 **Overtime** ($3,000) is recommended unchanged to fund expected overtime related to cyber security incidents or projects.

710106 **Stand-By** ($26,624) is recommended unchanged to fund Stand-By pay for network security staff. Due to increasing cyber threats after hours, on weekends, and holidays, it is necessary to have network security staff available for immediate response if necessary.

SALARIES & EMPLOYEE BENEFITS (continued)

710200 **Retirement** ($321,052) is recommended increased $ 79,058 to fund Retirement costs.

710300 **Health Insurance** ($121,736) is recommended increased $26 to fund Health Insurance costs.

SERVICES & SUPPLIES

720300 **Communications** ($6,000) is recommended increased $1,500 to fund the following:

FY 23-24	FY 24-25	Item
$4,500	$6,000	Cell Phone Service

720800 **Maintenance – Equipment** ($142,349) is recommended increased $64,849 to fund the following:

FY 23-24	FY 24-25	Item
Recurring Costs		
$25,000	$58,514	Cisco SmartNet & Security Licensing Cisco SmartNet ensures ongoing support and maintenance of network infrastructure equipment. SmartNet is critical to maximize the reliability, performance, and security of the County's network and support of critical constituent services, including Public Safety. The cost of SmartNet increases as network infrastructure equipment is added to the County network. In support of recent capital improvement projects, additional network equipment has been purchased, increasing Cisco SmartNet costs.
$2,500	$3,000	Storage Area Network (SAN) Licensing
$5,000	$4,300	Overland Maintenance
$45,000	$0	Backup Expansion
$0	$43,535	Network & Security Project Maintenance Agreements (Previously paid from Account 730330)

SERVICES & SUPPLIES (continued)

720800 **Maintenance – Equipment (continued)**

New - Recurring Costs

$0	$33,000	VMware Maintenance VMware facilitates the transition from physical servers to virtual ones, streamlining the technical infrastructure at the Sheriff's Office, by allowing multiple virtual machines to run on a single physical server. This not only conserves physical space but also enhances efficiency, agility, and scalability, enabling OoIT to better manage resources and reduce operational costs.

721300 **Office Expense** ($10,000) is recommended decreased $9,000 to fund the following:

FY 23-24	FY 24-25	Item
$15,000	$7,500	Back Up Tapes
$1,000	$2,000	Office Supplies
$1,000	$500	Training Materials
$2,000	$0	Office Furniture

721314 **Computer Equipment** ($5,000) is recommended decreased $11,000 to fund the following:

FY 23-24	FY 24-25	Item
$16,000	$5,000	Computer Equipment

721400 **Professional & Specialized Services** ($626,246) is recommended decreased $25,149 to fund the following:

FY 23-24	FY 24-25	Item
Recurring Costs		
$7,000	$7,000	Hard Drive Destruction

SERVICES & SUPPLIES (continued)

721400 **Professional & Specialized Services (continued)**

FY 23-24	FY 24-25	Item
$800	$500	ISACA Memberships
$61,250	$62,195	Cisco Talos Incident Response
$35,000	$20,000	Trace Digital Forensics Services
$68,845	$73,250	Cloud Back Up Service – Microsoft 365
$40,000	$40,000	Penetration Testing Remediation
$35,000	$35,000	Information Technology Service Management (ITSM)
$317,000	$225,000	Security Operations Center (SOC) Log Archive
$0	$117,471	Microsoft Premier (Previously paid from ORG Key 00243)
$0	$7,510	Network & Security Project Professional Services (Previously paid from Account 730330)
$14,000	$10,000	Data Center Cleaning Services
$16,000	$0	External Consulting and Support - Due to the County's continuous investment in training, this line item will be deleted for Fiscal Year 2024-25. Continued savings in this area is dependent on staff retention and continuous technical training.

One Time Costs

$5,000	$0	Backup Expansion Configuration
$20,000	$0	Mobile Device Management
$19,500	$0	Ransomware Protection Configuration Services
$12,000	$13,320	Redundant Backup Site Configuration
$0	$15,000	Data Loss Prevention (DLP) Planning & Analysis Pilot Program

721426 **Software** ($1,153,966) is recommended increased $337,971 to fund the following:

Software and Subscription costs generally increase each year. Although many factors may influence the cost of software and subscription services, the County is most impacted by manufacturer price increases and the overall County usage (number of employees, number of devices, number of records, etc.) of the software.

SERVICES & SUPPLIES (continued)

721426 Software (continued)

FY 23-24	FY 24-25	Item
Recurring Costs		
$22,237	$28,650	Manage Engine Active Directory Manager & Active Directory Audit Plus
$4,000	$4,200	AdminDroid
$25,000	$7,500	Azure Cloud Security – Multi Factor Authentication Tokens
$20,000	$15,000	Secure File Solution
$4,000	$4,200	Batch Patch Software
$22,000	$25,000	Integrated Electronics Badge Software
$85,000	$85,000	Internal Vulnerability Management & External Testing
$50,000	$57,250	Server Infrastructure Network Management System (NMS)
$20,814	$23,214	Manage Engine Desktop Central and Patch Manager
$50,000	$62,012	Network Infrastructure Monitoring & Mapping Maintenance
$4,000	$4,200	Secure Password Manager (IT) Subscription Service
$28,044	$33,497	Security Awareness Training
$275,000	$445,997	Microsoft Enterprise Agreement
$10,600	$10,600	SSL Certificate Renewal
$49,000	$51,550	Vendor Remote Access
$63,000	$71,500	Enterprise Backup Software – Annual License and Maintenance
$3,000	$6,000	Deploy & Inventory Software
$3,600	$16,750	Secure Browser
$2,650	$2,800	Certificate Tracking and Management
$0	$14,103	Network & Security Project Software (Previously paid from Account 730330)
$9,850	$10,050	Training Subscription Software
$30,000	$32,000	Service Management Licenses
$6,200	$0	Pen Testing

SERVICES & SUPPLIES (continued)

721426 **Software (continued)**

FY 23-24	FY 24-25	Item
New - Recurring Costs		
$0	$28,000	Countywide Password Manager
$0	$24,360	Malware Sandbox Safe Email Inspection & Analytics
$0	$38,200	Secure Email Domain Record Advancement
$0	$20,000	Firewall Licensing
$0	$12,275	Microsoft Teams Back Up
$0	$1,100	Azure Active Directory Auditing & Visibility
$0	$6,435	Exchange Online M365 Visibility
$0	$750	Vulnerability Tracking Project Software
$0	$9,272	Data Center Storage licensing
$0	$2,500	Security Camera Licenses

721500 **Advertising** ($2,000) is recommended increased $2,000 to fund recruitment advertising for security positions.

721900 **Property Tax** ($15,000) is recommended decreased $3,000 to fund the Property Taxes associated with the Network ￼and Security Project Lease

722002 **Transportation & Travel** ($51,190) is recommended increased $13,810 to fund training needs throughout the year.

Training increase of $13,810 is due to cybersecurity staff, requiring training on the County’s current strategies and technology. Moreover, with the increased utilization of Microsoft 365, staff will attend the Microsoft Insight conference for the first time. This provides an understanding of the Microsoft roadmap allowing the security team to mold a strategic plan around new features and releases.

FY 23-24	FY 24-25	Item
$6,000	$10,000	SANS Security
$16,525	$18,000	Cisco Live

SERVICES & SUPPLIES (continued)

722002 **Transportation & Travel (continued)**

FY 23-24	FY 24-25	Item
$5,190	$5,190	RSA Training
$0	$8,000	Microsoft Ignite
$0	$10,000	Cybersecurity Defense Training
$5,650	$0	BlackHat USA

OTHER CHARGES

730330 **Rent** ($335,596) is recommended decreased to $80,144 to fund the following capital lease:

FY 23-24	FY 24-25	Item
$415,740	$335,596	ConvergeOne Financial – Network Security Implementation Project (Final Payment: September 2028)

Some costs have been removed from Account 730330 and added to Accounts 720800, 721400, and 721426 due to GASB 87 Lease Reporting Requirements.

FIXED ASSETS

740301 **Equipment** ($104,101) is recommended decreased $40,899 to fund the following:

End-of-Life (EOL) equipment indicates it has reached the end of its “useful life” and will no longer market, sell, or update. This introduces risk to the availability of the connectivity the device provides. In addition, the system becomes more insecure day by day leaving additional areas of vulnerability throughout the enterprise.

FIXED ASSETS (continued)

740301 **Equipment (continued)**

Replacement Equipment

The existing firewall infrastructure located at the Coroner's Office, the County Clerk-Recorder's Office, and the Tesoro Viejo Fire Station will each reach the end of its operational life which can pose significant risks to the security and integrity of critical data and communication channels if not replaced. The firewall replacement is essential to fortify our network security and ensure the continued protection of sensitive information. This project is for the replacement of the hardware, configuration, and implementation of the devices to keep them in-life and in compliance while maintaining support.

$25,700	Coroner's Office Firewall Replacement – End-of-Life
$25,700	Clerk-Recorder's Office Firewall Replacement – End-of-Life
$25,700	Tesoro Viejo Fire Station Firewall Replacement – End-of-Life

In 2018, the Office of Information Technology (OoIT) highlighted to the Board the pressing issue of technical debt, with over 80% of the network infrastructure being end-of-life. Through the Board's support, we've since adopted a replacement strategy to prevent such issues, incorporating substantial investments in software firewalls to reduce the need for physical ones, though specific scenarios still necessitate their use. The replacement equipment listed above are examples where physical hardware is situationally required.

New Equipment

A fireproof LTO (Linear Tape-Open) safe serves the purpose of providing secure storage for LTO tapes in the event of a fire. LTO tapes are magnetic storage media commonly used for backup and archiving data. These tapes are sensitive to heat and can be damaged or lose data if exposed to high temperatures during a fire. The use of a fireproof LTO safe is a crucial part of a comprehensive data protection and disaster recovery plan, ensuring that critical data stored on LTO tapes remains intact and recoverable even in the face of a fire emergency. In addition, during a recent external audit, lack of a fireproof LTO safe was identified as a finding.

$27,000	Data Commander Fireproof Linear Tape Open (LTO) Hard Drive Safe

COUNTY OF MADERA
BUDGET UNIT POSITION SUMMARY
BUDGET FOR THE FISCAL YEAR 2024-25

Department:	**Information Security**
	00243
Function:	**General**
Activity:	**Other General**
Fund:	**General**

		2023-24 Authorized Positions		**2024-25 Proposed Positions**		**Y-O-Y Changes in Positions**		
JCN	**CLASSIFICATION**	**Funded**	**Unfunded**	**Funded**	**Unfunded**	**Funded**	**Unfunded**	**Notes**
3387	Network Security Engineer I or	**5.0**	**-**	**5.0**		**-**	**-**	
3388	Network Security Engineer II							
4121	Deputy CIO - Network & Security Services	**1.0**	**-**	**1.0**		**-**	**-**	
3387	Network Security Engineer I or							
3388	Network Security Engineer II or							
3389	Senior Network Security Engineer	**1.0**	**-**	**1.0**		**-**	**-**	
4222	Executive Assistant to the Dept Head	**1.0**	**-**	**1.0**		**-**	**-**	
	TOTAL	**8.0**	**-**	**8.0**	**-**	**-**	**-**	

NOTES: