Cybersecurity Protection Plan

Security Information Event Management (SIEM)

Network Security

Endpoint Detection & Response (EDR)

Vulnerability Management

Managed Defense & Response (MDR)

Email Security

Backups

External Services

Risk Assessments

Framework for TVCC's Cybersecurity Initiative in FY 2021-22

Treasure Valley Community College has an ongoing need to improve and evolve its cybersecurity preparedness. The Information Technology department has discussed a range of options that could be the focus of its efforts during the 2021-22 fiscal year, and from those conversations have prepared the following framework document for consideration by the TVCC Executive Team.

Attached as an appendix is an audit tool for cybersecurity developed by Scott Carpenter which describes the major components of a comprehensive cybersecurity plan. The benefit of this tool is that it gives a clear set of choices for TVCC to prioritize, and we have used it as a roadmap for this framework.

In general, it is possible to segment the components of a cybersecurity plan into two groups – those initiatives which would require significant financial outlay, and those which generally rely more on employee work and review than expense with outside vendors. Differentiating and prioritizing these components is critically important to any conversation of cybersecurity, and readers are **strongly urged to read Appendix A** to get a deeper understanding of their definitions. In any case, the two groupings are:

Initiatives involving expense and external partnerships with vendors

1. Network infrastructure security
2. Endpoint Detection and Response (EDR)
3. Vulnerability and Patch Management
4. Managed Defense and Response (MDR)
5. Email systems security
6. Backup solutions
7. External Assessment Services
8. Security Information Event Management (SIEM)
9. Security Awareness Training (this also exists in the other grouping, because it is possible to develop a "home-grown" training solution, if so desired.)

Initiatives which primarily involve TVCC employee labor

10. Security Policy Framework (this framework must include policies on backups, as well as cybersecurity and incident response)
11. Risk and Gap Assessments
12. Security Awareness Training

TVCC began working on its cybersecurity initiative beginning in the summer of 2018 by engaging CompuNet, an IT Services vendor located in Boise, to do an IT security gap assessment. The results of that assessment found TVCC had elements of information security in place, but that no holistic plan or set of solutions had been implemented. Since that time, the TVCC IT Department has been implementing various systems and solutions recommended by the gap assessment, but we continue to have shortcomings which need to be addressed.

Additionally, in 2020, TVCC had a cybersecurity incident which tested the IT Department's disaster recovery planning and backup systems. Though the existing backup systems and routines held up well,

the experience helped identify additional shortcomings in the department's preparedness and disaster recovery policies. The learning from that incident has further influenced the ongoing security initiative.

Existing solutions

TVCC has already put in place systems and processes which address some of the previously described list of cybersecurity initiatives. Some of the existing solutions are transitional, while others are more mature and tested. For each solution, we include an internal assessment of the existing systems' "maturity" – that is, how broadly and effectively the solution has been addressed and implemented. Solutions which we deem "mature" probably will not need to be reassessed or improved in the upcoming two fiscal years, while those that are "immature" or "aging" may need improvement or replacement, depending on the current conditions of cybersecurity threats.

- ### Network security
  TVCC has a well-developed installation of network firewalls and edge security solutions. The College uses Palo Alto Networks firewalls and a suite of anti-virus, anti-malware and URL filtering subscriptions to check all inbound and outbound traffic on the staff and student networks. There is no expectation this solution will need to be replaced in the next five years, but configuration improvements and changes driven by changes in the College's needs are likely.
  Assessed Maturity Level: **Mature**

- ### Endpoint Detection and Response (EDR)
  TVCC uses the Palo Alto Cortex XDR software as its EDR solution. Formerly known as Traps, the system serves as an anti-malware agent installed on every computer (physical or virtual) on the College network; it prevents the unauthorized installation of software and also serves to alert administrators when a device begins to exhibit unusual activity.
  Assessed Maturity Level: **Mature**

- ### Vulnerability and Patch Management
  Currently the College is transitioning from one Microsoft package for managing software patches – the existing WSUS Server is being replaced by a more capable system called InTune.
  Assessed Maturity Level: **Immature**

- ### Backup solutions
  The IT Department uses a layered backup solution. Its initial backups are made on the department's Pure SANs, where hourly snapshots of the servers are made. These backups are augmented using software provided by Veeam to manage the backup processes of its server infrastructure, which is complete virtual within a VMWare server infrastructure. The backup files made by Veeam are stored to redundant storage locations on a large storage SAN hardware; the department has multiple devices located in Ontario and Caldwell. Additionally, monthly archives of the backup files are maintained on a separate SAN, and also through cloud storage, in order to provide record retention and forensic discoverability.
  Assessed Maturity Level: **Mature to Aging**

- ### External Assessment Services
  The IT Department has begun the process of implementing external assessments of its public-facing network; a contract has been established with CISA to provide reports on any vulnerabilities found on the College's public websites, servers, etc. An initial review by CISA yielded a list of roughly 80 insecurities in College servers, most of which have now been mitigated. Future plans for this initiative will involve expanding the assessment services to include active penetration testing.
  Assessed Maturity Level: **Immature**

- ### Security Awareness Training
  The IT Department has deployed security training through an online tool provided by Proofpoint. The system provides employees online training and simulations about current threats, and has the ability to allow the IT department to conduct phishing simulations and other tests of the employees' awareness of unsafe security behavior.
  Assessed Maturity Level: **Immature**

- ### Security Policy Framework
  The College is currently in the process of reviewing and improving the policy framework used to govern cybersecurity. Several new policies have been developed recently – policies which cover areas such as incident response and information security – and a number of additional policies have been identified for future development.
  Assessed Maturity Level: **Immature**

- ### Risk and Gap Assessment
  It was a gap assessment initiated by the IT Department which really kicked off the College's cybersecurity initiative in 2018. As was previously described, the assessment used the Center for Internet Security's Top 20 Critical Security Controls to identify shortcomings and needed improvement in the College's technology systems. The IT Department has been working to address the findings of the assessment and expects within a year to 18 months to revisit and re-conduct the gap assessment process.
  Assessed Maturity Level: **Aging**

- ### Managed Defense and Response
  The IT Department currently has a subscription to Palo Alto Networks' managed threat hunting services. This service reviews the College's firewall logs on a daily basis for any known security issues.
  Assessed Maturity Level: **Immature**

- ### Security Information Event Management (SIEM)
  The College currently pays for one terabyte of cloud storage on Palo Alto Networks' Cortex Data Lake. This collects logs from the College's firewalls and from the Cortex XDR software running on the network endpoints. There may need to be an expansion of this storage, or a different SIEM

solution may also be needed in the future.
Assessed Maturity Level: **Immature**

- ### Email system security
  Currently the College uses only the default protection from the Microsoft Office 365 suite under the A3 plan.
  Assessed Maturity Level: **Aging**

New initiatives and proposed solutions

Because of the shifting and evolving nature of cybersecurity threats, the College's existing list of cybersecurity solutions will never be "complete" or without need of continued improvement. That said, the previous listing of initiatives represents a significant investment of time and money to protect the College community, and the IT Department feels confident enough in most of those solutions to maintain them into the future; the department is now turning its focus to several new initiatives and iterating on several other existing solutions.

From this list, we have identified the following initiatives to focus on immediately – this doesn't eliminate the others are areas of concern but does mean they may be pushed back in order of priority. These are loosely arranged by order of priority, though these may be reordered after evaluation by College leadership:

- ### Managed Defense and Response
  The IT Department lacks both the staffing and expertise to effectively monitor all aspects of the College's security needs. This sort of monitoring is the area of expertise of companies offering "Security Operations Center as a Service", and the College leadership has directed the IT Department to identify, evaluate and implement a SOCaaS as soon as possible. This is the primary cybersecurity initiative for the College to add in FY 2021-22**.**

- ### Backup solutions
  The IT Department identified several internal issues with its existing backup solution in the aftermath of 2020's security incident, so it has been moving to address those shortcomings. Several additional backup devices will be added, and these devices are better designed to prevent some of the data corruption and encryption seen in a typical ransomware attack. The new devices will also have increased recovery speeds which would help speed a recovery in the case of another future security breach.

- ### Vulnerability and Patch Management
  Identifying and fixing software security issues is a task with many parts – a comprehensive solution involves both the secure configuration and deployment of computers, software and other network devices, as well as processes for searching for existing installations which need to be patched or updated. The IT Department has decided to begin addressing this initiative by replacing some older tools with a new solution from Microsoft called InTune, which is intended to automate the deployment and management of computers and software. The department

expects that once InTune is fully implemented, additional tools may be needed to search for weaknesses in devices which aren't desktop computers or laptops. It should also be noted that TVCC has purchased the Host Insights option from Palo Alto for the Cortex XDR client; this add-on broadens the capability of the EDR client to help identify host vulnerabilities.

- Security Policy Framework
  The IT Department has devoted significant effort to looking for improvement to the College's policies which cover cybersecurity, including reviewing of similar policy development at our sister institution, Southwestern Oregon Community College. Some policies have been advanced to the College leadership, while others are still being refined; the goal is to bring as many policies to completion during FY 2021-22 as possible.

This represents the dividing line between those initiatives which have the highest priority and focus currently for the IT Department; the following items have some activity or focus, but may be deprioritized or changed as other College priorities demand.

- Email security
  Email continues to be one of the most effective ways for bad actors to attack College systems. While the Microsoft 365 system has a certain level of anti-virus protection, it does less to prevent phishing and more sophisticated advanced persistent threats. Addressing these concerns generally requires additional partnerships, and while the IT Department has begun evaluating potential solutions, funding for these systems was not included in the FY 2021-22 budget, so department leadership expects to present a recommendation for the FY 2022-23 budget process.

- Risk and Gap Assessment, specifically targeting "Internet of Things" devices
  A significant new area of security concern for the IT Department is the increasing presence of "Internet of Things" (or IOT) devices which connect to the College networks but which don't really have easily managed software or configurations. Examples of this sort of device would be a Sony Playstation or Microsoft Xbox, or the "Smart" televisions which are increasingly common – these devices make heavy use of connections to the Internet, but there really isn't an "operating system" that the end-user (or IT Department) can access to harden its security. Instead, for the IT Department, the task boils down to identifying those devices when they're added to College networks, and then segregating their access so they can't be used to launch attacks on the rest of the campus. This is a new area of concern for us, and isn't limited only to equipment owned by students – increasingly equipment such as HVAC controllers and door locks are also on our networks, and those devices are primarily the responsibility of College departments.
  The IT Department does not yet have clear responses to this area of challenge, so a first step will be to do a risk assessment and explore possible management responses. Preliminarily, we expect to add a new service from Palo Alto Networks which would augment the College firewalls' ability to specifically identify IOT devices. As the IT Department looks toward its next full gap analysis, we expect the IOT issue to be one of the major focuses of that effort.

- ### Security Information Event Management (SIEM)
  The IT Department expects to continue increasing storage capacity and collecting log information from more systems. An expected enhancement will be to add logs for network access when users log into devices on campus; currently, the existing logging focuses more on the activity of network devices, rather than users, but both types of record are critical for forensic discovery in the case of a cybersecurity incident.

- ### Network Security
  The IT Department expects to continue segmenting networks and improve a Zero-Trust model of network design, where all devices on a network have only the access they need to operate. The Department also expects to research additional subscriptions that might improve perimeter security – for example, protecting the College's DNS records from being hijacked by an external bad actor.

- ### Endpoint Detection and Response (EDR)
  While the Palo Alto Cortex XDR endpoint solution has been fully implemented throughout College devices, the IT Department expects to continue working with consultants to improve the software's rules for monitoring and blocking more unknown threats.

- ### Security Awareness Training
  The IT Department and College Leadership team will need to continue working to get more employees to complete this training. If we can raise the adoption rate among staff, we may seek to expand the training to include students.

- ### External Assessment Services
  As stated above, the IT Department has engaged an external vendor to begin providing review of the College's networks from the outside. We expect to continue this review, but will also attempt to determine how those services can be broadened and improved once we have greater experience working with findings that are provided to the Department.

Future Initiatives

This document really only represents a snapshot in time – the threats and challenges of cyber security are constantly evolving. The IT Department is already beginning to consider new initiatives, or expansions of existing ones, to address anticipated changes. Examples of future areas of concern include:

- Expansion of the College's Managed Defense and Response solution to include the Microsoft 365 systems; currently our MDR looks mainly only at on-premise network assets, but we will want to monitor activity at our cloud infrastructure as well.
- Cloud VPN and Firewalls. As the College moves more operations to cloud infrastructure, we will need to harden those systems, and some solutions may include installing virtual networks (VPNs) or virtual firewalls in front of those solutions to provide protection.

- Virtual Desktops in the cloud. TVCC currently uses virtual desktops for student and staff use throughout the campus, and these desktops were an important part of the COVID-19 response as well. In the future, the IT Department expects to move from on-premise hosting hardware for these virtual desktops to cloud-based hosting. This should offer better performance and security for off-campus users, a group we expect to increase in the future.
- Funding for cybersecurity expertise. TVCC will likely be challenged to find and afford dedicated security individuals as college employees – their salary expectations are simply too high to be budgetarily possible. Instead, TVCC and IT leadership will need to budget for the external consulting services needed to augment our internal capacity.

Conclusion

It is always challenging to reduce such a broad and complex technical area as cybersecurity into even an 8- or 10-page summary. The TVCC IT Department appreciates the care other College stakeholders have given to reading and understanding these issues – it's not possible for the IT Department to be the sole owner of the topic, so we recognize and appreciate the reader's dedication to the questions raised here. TVCC's entire community is stronger because of that dedication – thank you.

Appendix A - Cybersecurity Component Descriptions

What is cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. Any cybersecurity program is going to be composed of a layered set of components which work together to address various ways an institution can be attacked. What follows is a list of components and descriptions of how they contribute to a holistic institution-wide solution.

Network Security:

Includes Firewalls and subscription licenses to protect the network, as well as all related assets, data and users from cyberattacks and nefarious activity. Includes a combination of preventative and defensive measures designed to deny unauthorized access of resources and data.

Endpoint Detection & Response (EDR)

Security software for endpoints (desktops, laptops, and mobile devices) to process and protect devices in real-time against malicious activity and provide logging to other security platforms.

Security Awareness Training

Resources to help your users understand the key role they play in helping to protect an organization's data and other key assets. It also educates them on threat tactics, social engineering, and the scams used to gain access to secured resources. Helps improve users' ability to spot malicious content before they become a victim.

Vulnerability Management

These systems focus on issues in software, hardware, open ports, and software configurations. They attempt the discovery of weaknesses or other conditions in an organization that a threat actor, such as a hacker, nation-state, disgruntled employee, or other attacker can exploit to adversely affect data security.

Managed Defense and Response (MDR)

Providers 24/7 threat monitoring, detection and response services to customers leveraging a combination of technologies deployed at the network and endpoint. Includes advanced analytics, threat intelligence, and access to a pool of security researchers and engineers, who are responsible for monitoring networks, analyzing incidents, and responding to security cases.

Security Information Event Management (SIEM)

SIEM software works by collecting log and event data generated by an organizations application, security devices and host systems and bringing it together into a single centralized platform. SIEM gathers data from antivirus events, firewall logs and other locations; it sorts this data into categories for better analysis.

Email Security

Software or service for protecting email accounts, content, and communication against unauthorized access or compromise. Includes alerts for access based on location, phishing attacks and provides data loss prevention (DLP). Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. Email is also a common entry point for attackers looking to gain a foothold in an enterprise network and obtain valuable company data.

External Services

Outside provides who monitor and preform periodic test against organizational resources. Examples of services are penetration testing, monitoring dark web for data leaks, identify all your Internet facing assets.

Risk Assessments

Identifies the various information assets that could be affected by a cyber-attack through a GAP analysis. Develop policies and procedures to detect, respond to, and recover from network security incidents. These types of plans (Incident Response Plan) address issues like cybercrime, data loss, and service outages that threaten daily work.

Backup strategies and Policies

Provide guidelines for the continuity, restoration and recovery of data in the event of an equipment failure, intentional destruction of data or natural disaster. Manage a backup strategy such as the 3-2-1 method. The 3-2-1 backup strategy simply states that you should have 3 copies of your data on two different media, with one copy off-site.

Cybersecurity Component Audit Tool

Security Policy Framework	Backup Strategies & Policies	Risk/Gap Assessement	Network Security	Endpoint Detection & Response (EDR)	Security Awareness Training	Vulnerabilty Management	Managed Defense & Response (MDR)	Email Security	Security Information Event Management (SIEM)	External Assessment Services	
$ 10,000	$ 20,000	$ 5,000	$ 30,000	$ 25,000	$ 8,000	$ 25,000	$ 85,000	$ 35,000	$ 25,000	$ 15,000	**Estimated Cost**
9	3	10	1	2	6	7	5	4	8	11	**Priority (Order by number)**
Medium	Critical	Low	Critical	High	Medium	Low	High	Critical	Medium	Low	**Risk**
											Required by?
Yes[2]		Yes[2]	Yes[3]	Yes[3]	Yes[3]	Yes[3]	Yes[3]		Yes[3]	Yes[3]	**GLBA**
Yes[1]		Yes[1]	Yes[1]	Yes[1]	Yes[1]		Yes[1]				**Title IV**
? - TVCC has not yet received explicit directives from our insurer regarding required cybersecurity components											**Insurance Company**
? - We're really unsure if there are ORS that are applicable. More research is needed.											**State ORS**
Partial	Partial	Yes	yes	Yes	Yes	Yes	No	No	Partial	Yes	**Is component in place?**

Total Estimated Cost of all Components FY2021-2022	**$ 283,000.00**

[1] Title 16 → Chapter I → Subchapter C → Part 314.4

[2] GLBA → Title V → Sections 501 and 505

[3] NIST SP 800-171 Rev. 2 -> Section 3.1 - 3.14

Category	Vendor	Price	In Place at TVCC	Description
Network Security	Palo Alto	28,706.26	Yes	Annual support Contract & Annual subscriptions for all firewalls
Endpoint Detection & Response (EDR)	Palo Alto	19,576.00	Yes	Cortex XDR Pro for 800 end points
Security Information Event Management (SIEM)	Palo Alto	4,882.78	Partial	1 TB of Cortex Data Lake storage
Vulnerability Management	Palo Alto	5,744.00	Yes	Host Insights add on for Cortex XDR Pro
Security Awareness Training	ProofPoint	8,206.38	Yes	Includings training for staff only. Students are not part of this system
Managed Defense and Response (MDR)	Critical Start	35,600.00	No	Phase I: New service start up in September includes 14 month contract. Works with our existing Cortex products. Phase II: Add on service to cover protection for Office 365
Backup Strategies & Policies	Veeam, Wasabi, ExaGrid	17,513.00	Partial	Includes only annual costs for software, support and cloud storage. Does not include the cost of the physical hardware
External Monitoring	CISA, Palo Alto	6,968.00	Yes	Includes Palo Alto Managed Threat Hunting service and signed up to use CISA free service for Hygine Reporting. (Includes PEN testing, Website monitioring and vulnerability scanning)
Risk/Gap Assessement	Compunet	2,000.00	Yes	Covers support from CompuNet engineers to review Firewalls and make recommendations
Security Policy Framework	Eric Ellis	2,000.00	Partial	Covers consultant hours to develop policies, procedures and documentation
Email Security	Mimecast	34,321.88	No	Includes all services for 437 employee accounts and basic coverage for 4600 student accounts
Total annual cost of all Cybersecurity products		**$ 165,518.30**		Current Cybersecurity budget for FY2021-2022: $105,170.00

Notes:

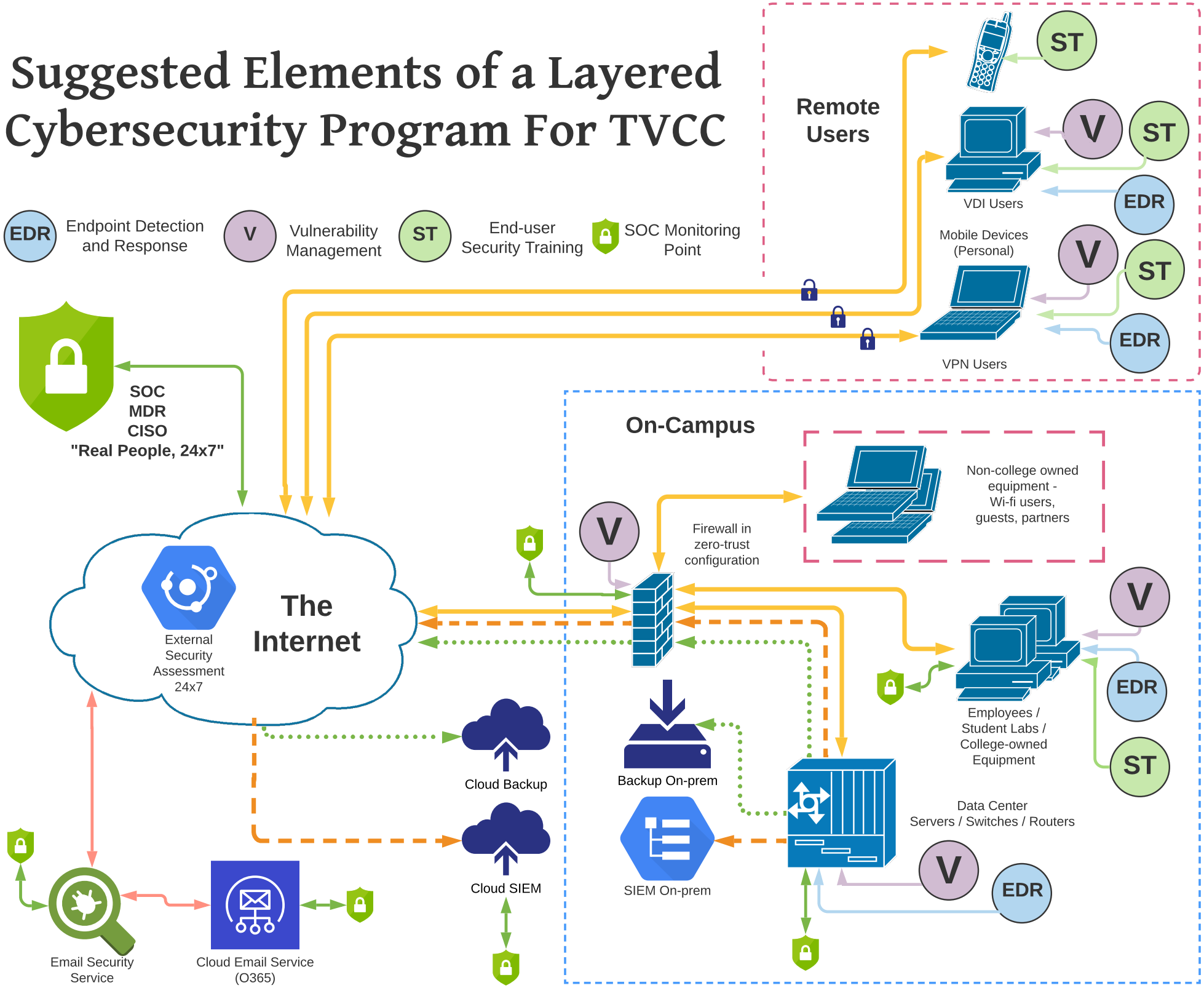
** Only includes annual costs for Cybesecurity products and services*

** Does not include any install or setup costs*

** Does not include any personnel costs*

** Does not include any hardware costs for new or replacement equipment*

Suggested Elements of a Layered Cybersecurity Program For TVCC



2021 Cybersecurity Goals & Projects

- Security policy frame work
  - Finish IR Policy
  - Finish IR plan
  - Drafts are complete
- Risk and gap assessment
  - Limiting access to management systems from IT
  - Removing unsecure protocols and access
  - Research IoT and how to secure
- Backup solutions
  - Implement 3-2-1 Method
  - 3 copies of your data, 2 different media types, 1 off-site
  - Purchased two new 72 TB ExaGrid Systems
  - Repair older 27 TB Quantum Units
  - Setup Wasabi cloud service
- Security awareness training
  - Setup 3 different employee training modules
  - Week before each term (Fall, Winter, Spring)
- Vulnerability management
  - Added Palo Alto Host Insight service (Already in place)
  - Working on Microsoft Intune for patch management
- Network security
  - Adding new network access for special systems (Book store, food services, EOU, SimMan)
  - Adding SSL decrypt for TVCC websites
- Endpoint detection and response (edr)
  - Monitoring traffic weekly and looking for security issues.
  - Push more users toward MFA
- External Services
  - Signed up with CISA for free services
  - Weekly reports for Cyber Hygiene
  - Weekly reports for Web Application Scanning (WAS)
- Managed Defense and Response (mdr)
  - Phase I – Add monitoring for End points and Network (Looking to roll out project in October or November)
  - Phase II – Add monitoring for Office 365 Email (After January or July)
- Email security
  - Turn on DLP from Microsoft Cloud
  - Researching Email security solutions