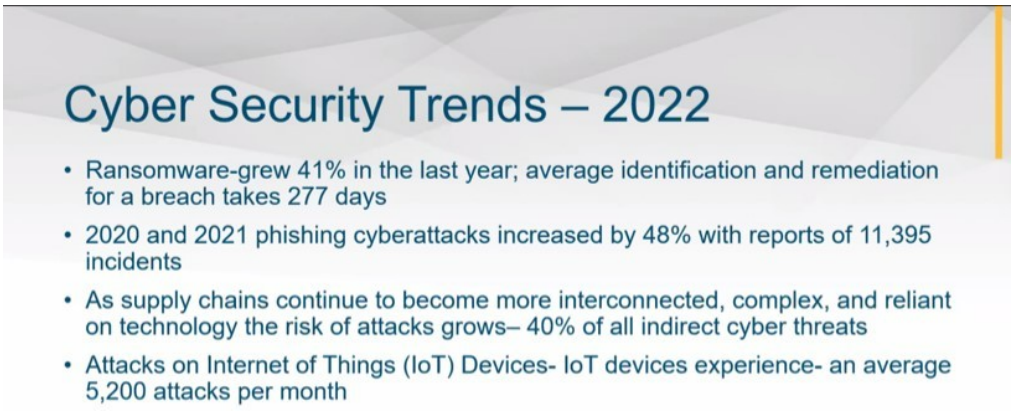
Cyber Center Program Proposal

Need: Businesses of all sizes need assistance with Cyber Security challenges. Tools such as broadband and information technology can help small businesses reach new customers and increase their efficiency and productivity. Training employees, protecting customer information, and preventing cyber-attacks (11,395 incidents/year) are necessary for all businesses, regardless of size.

As large industry/government entities tighten up controls, bad actors are increasingly targeting supply chain companies (40%). These challenges are more costly for small and mid-size businesses as they limited financial resources compared to larger organizations. These business owners are likely seeking the information and implementing those directives themselves versus hiring an "expert" to assist.

Trends in Cyber Security challenges like those listed below demonstrate the need to assist small to mid-size businesses in learning about Cyber Security and how to protect their information.



https://www.afsbirsttr.af.mil/About/Cybersecurity-and-the-Blue-Cyber-Education-Series/
https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/
https://www.cisa.gov/cyber-guidance-small-businesses

The Cyber Center Program will provide educational seminars and one-on-one advising to small and mid-size businesses who need assistance with developing and implementing process and procedures to secure the safety of their business information. The Cyber Center at Del Mar College would provide training and advising resources to businesses who need the following assistance:

- Cyber hygiene protocols
- Protect customer information, business intellectual property, staff information
- Compliance to do business with large industry & government (CMMC Level I – IV)
- Protection from ransomware attacks (increased 41% in 2022)
- Website optimization

Programing: The program will primarily focus on one-on-one advising, both virtual and in-person, as each business's needs are specific and individual. One-on-one advising with a trained program manager will allow for the identification of potential challenges and recommendations specific to that business's need and ability to implement. In addition, the program will provide workshops to larger groups for more generalized cyber security information.

The program will be marketed to small businesses through established training events including APEX and CRC, marketing to identified stakeholders, and referrals from network partners. Plans are to develop a dedicated webpage to which the marketing materials will drive traffic for more information about the program.

Cybersecurity is mentioned in both the APEX and CRC programs as part of the mission requirements to inform clients about relevant business challenges. Unfortunately, current staff in these programs do not have the necessary IT experience to assist clients. Instead, clients are directed to online cybersecurity resources. With the development of the Cyber Center Program, these clients will be directed to actual staff and workshops with the relevant IT background to support client needs.

The program could begin delivering client advising and workshops within three to six months of funding. Pre-program delivery tasks include hiring the program manager, developing collateral materials, establishing a webpage, developing the training curriculum and training aids, establishing referral networks with other programs and resources, and identifying additional expert consultants as needed to address specific client challenges.

Goals: Fifty (50) one-on-one clients with an estimated average of 7 hours of advising depending on need (range between 1-15 hours). Sixty (60) workshop clients with a target of four (4) workshops (virtual/in person) estimating 15 attendees on average.

Personnel Needs: The Cyber Center will need one (1) full time Program Manager with skills levels equivalent to Information Security Analyst Level III at an estimated $96,200 for salary and benefits. In addition, the program would budget $25,000 for expert consulting support (500 hours @ $50.00) to address specific client needs beyond the scope of the Program Manager. Experts could include website developers and Cybersecurity Maturity Model Certification (CMMC) experts.

DMC Support: The College will provide office space for program personnel as well as training and meeting spaces for program delivery to clients. Additionally, the College will provide IT support including cyber security processes adapted for use by for profit businesses.

Estimated Cost: $126,200

Total estimated cost of the grant would be $126,200 which includes the following:

- Salary = $96,200 ($74,000 salary +$22,200 benefits)
- Expert consulting hours: $25,000 (500 hours @$50)
- Start up and equipment: $5,000

Basic Cyber Hygiene Best Practices for Businesses

- Enable 2FA authentication on all computers and devices.
- User name and password required to access all computers and devices.
- Anti-virus software is kept up-to-date.
- Equipment and devices no older than three years without active system updates enabled.
- Networks/servers strongly encouraged for companies sharing files across computers, devices.
- No computer or device can be used if system updates are no longer available.
- Cloud storage of files, file transfer or sharing must be secure from hackers and provide proof.
- File sharing applications (Google Drive, Dropbox, etc.) must be password protected.
- Website design and web hosting vendors must provide proof of security and hardening.
- Install software, application and hardware updates immediately when made available.
- Develop system security plan.
- Develop and execute plan of action and milestones.
- Develop and implement cyber incident reporting capability.
- Catalog and maintain list of equipment and devices.
- Evaluate the flow of documents and files in your business, their lifecycle and disposal.
- Ensure subcontractors, anyone you share data with are abiding by same protocols.
- Do not click on texts, links, attachments or anything else sent by an unknown, suspicious sender or on social media.
- Regularly restart computers and devices.
- Quarterly/bi-annually clear browser cache, delete temporary files, clear history.
- Do not store account log-in, credit card or other personal/company information in web browsers.
- Use a password randomizer and manager to generate and store strong passwords, do not use same passwords across multiple accounts, websites, etc. (Last Pass, 1 Password, Dashlane).
- Purchase a domain for your company website and e-mail, do not use free e-mail providers.
- Obtain scalable security solutions (Office 365, Google G Suite for Business, Windows 10 Pro).
- Develop processes to safeguard personally identifiable information, methods of payment, business and financial information, intellectual property.
- Perform routine system and file back-ups daily, weekly, monthly.
- Use an enclave if specific employees only need access to certain files not needed by everyone else.
- Designate a cyber compliance champion to lead company's efforts and provide training at least on an annual basis.
- Use only reputable IT providers, preferably certified in specific systems, hardware, software.
- Perform periodic drills with different security scenarios, evaluate response and what happened.
- Regularly empty trash cans – recycle bins and e-mail folders.
- Physically secure external storage devices when not in use.

- Reset default internet router password, create strong one and provide guest Wi-Fi network for non-employees.
- Revoke employees' access to company computers and devices immediately upon termination, leaving employment.
- Do not allow other individuals to use any employee's computer, devices.
- If you have a server/network, obtain utilization software to monitor potential breaches.
- Do not write down passwords or store in easily accessible locations.
- Do not use the same password repeatedly across multiple log-ins, reset every quarter.
- Limit employees to only access those systems, roles, applications, programs, files they need and are allowed to view to do their jobs.
- Control, manage connections between your company and outside networks.
- Avoid using public/free Wi-Fi internet.
- Control, limit employees' personal devices, computers from accessing company network, files, information.
- Know who has access to publish information on company systems, limit and control information posted.
- Assign individual, unique identifiers to employees, devices wanting to access your system, files – confirm identities before allowing access and verify user or device before granting access.
- Change any default, manufacturer-assigned user names and passwords immediately.
- Properly destroy and dispose of any storage media no longer used, needed – store in secure location when not being accessed.
- Consider using a firewall to protect against nefarious internet breaches.
- Consider purchasing IT support from retailers or consultants.
- Enter website addresses directly into browser address bar and not via search tool.
- Lock your computer and devices when not in use.