COMMITTEE AS A WHOLE
ZOOM MEETING OF THE BUSINESS AFFAIRS COMMITTEE OF THE BOARD OF TRUSTEES
Community College of Philadelphia
Thursday, October 7, 2021– 9:00 A.M.

TO: Members of the Business Affairs Committee of the Board of Trustees

FROM: Jacob Eapen

DATE: October 1, 2021

SUBJECT: **Business Affairs Committee (Committee as a Whole) Meeting**

A Zoom meeting of the Business Affairs Committee (Committee as a Whole) is scheduled for **Thursday, October 7, 2021 at 9:00 A.M.** The Zoom information for the Public Session follows:

PUBLIC SESSION
AGENDA

Topic: Business Affairs Committee Meeting: Public Session
Time: Oct 7, 2021 09:00 AM Eastern Time (US and Canada)
Join Zoom Meeting
https://ccp.zoom.us/j/93393177711?pwd=bzdLTUJTWnNqTzFMbFVrMGdKcllPQT09
Meeting ID: 933 9317 7711
Passcode: 8029
One tap mobile
+13017158592,,93393177711# US (Washington DC)
+13126266799,,93393177711# US (Chicago)

(1) Cyber and Infrastructure Security Presentation (Information Item)

This presentation provides a background of cyber security trends and what tools and services CCP has in place to enhance our security protocols to prevent unauthorized system access, protect critical information, and respond to cyber threats by adopting best practices.

This field is becoming increasingly significant due to the increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things."

Cybersecurity is the protection of computer systems and networks from information disclosure, theft of or damage to the hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. Like other institutions, at CCP, we will never have one silver bullet to completely reduce the risk of a cyber-attack but rather multiple technologies and processes in place to help ensure those threats are minimized.

One of our key strategies is the creation of a zero-trust approach to security that comprises of four principles: no user should be trusted by default since they could be compromised; VPN and firewalls can't do it alone since they just guard the perimeter; identity and device authentication should take place throughout the network rather than just on the perimeter; and micro-segmentation really helps minimize damage from hackers by creating interior walls and locks. Attachment A includes the presentation.

EXECUTIVE SESSION

An Executive Session will follow the Public Session. The Zoom information for the Executive Session follows:

Topic: BAC Executive Session
Time: Oct 7, 2021 09:30 AM Eastern Time (US and Canada)
Join Zoom Meeting
https://ccp.zoom.us/j/94973488159?pwd=ckQ1aEM0UVdkd3UrUVVDcTlTb1RmQT09
Meeting ID: 949 7348 8159
Passcode: BAC
One tap mobile
+16465588656,,94973488159# US (New York)
+13017158592,,94973488159# US (Washington DC)

(2) Next Meeting:

The next regularly scheduled meeting of the Business Affairs Committee will be held on Wednesday, October 20th at 9:00 A.M.

JE/lm
Attachments
c: Mr. Jeremiah White
Dr. Donald Generals
Ms. Marsia Henley
Mr. Gim Lim
Mr. Derrick Sawyer
Mr. Vijay Sonty

ATTACHMENT A

Cyber & Infrastructure Security Presentation

Community College of Philadelphia
www.ccp.edu

Cyber & Infrastructure Security - Background

83% of cyber security professionals say that their expanded infrastructure has complexified security challenges.

Forrester

Just 29% of organizations are monitoring unusual activity across their cloud and SaaS environments

Cybersecurity Insiders:
2020 Insider Threat Report

94% of cyber-attacks start with an email

"The COVID-19 pandemic accelerated the adoption of collaboration and cloud technologies as the world rapidly scaled up home working... this could heighten the cyber-resilience deficit where cybersecurity capacity is insufficient."

World Economic Forum

CYBERSECURITY

INFRASTRUCTURE SECURITY

- SaaS Takeover
- Rise of Fearware
- Server-Side Attacks
- Ransomware

Community College of Philadelphia
www.ccp.edu

2021 Top 15 Cyber-Threats Landscape

Malware, commonly referred to as "malicious software," is a term that describes any program or code that harmfully probes systems. The malware is designed to harm your computer or software and commonly masquerades as a warning against harmful software.

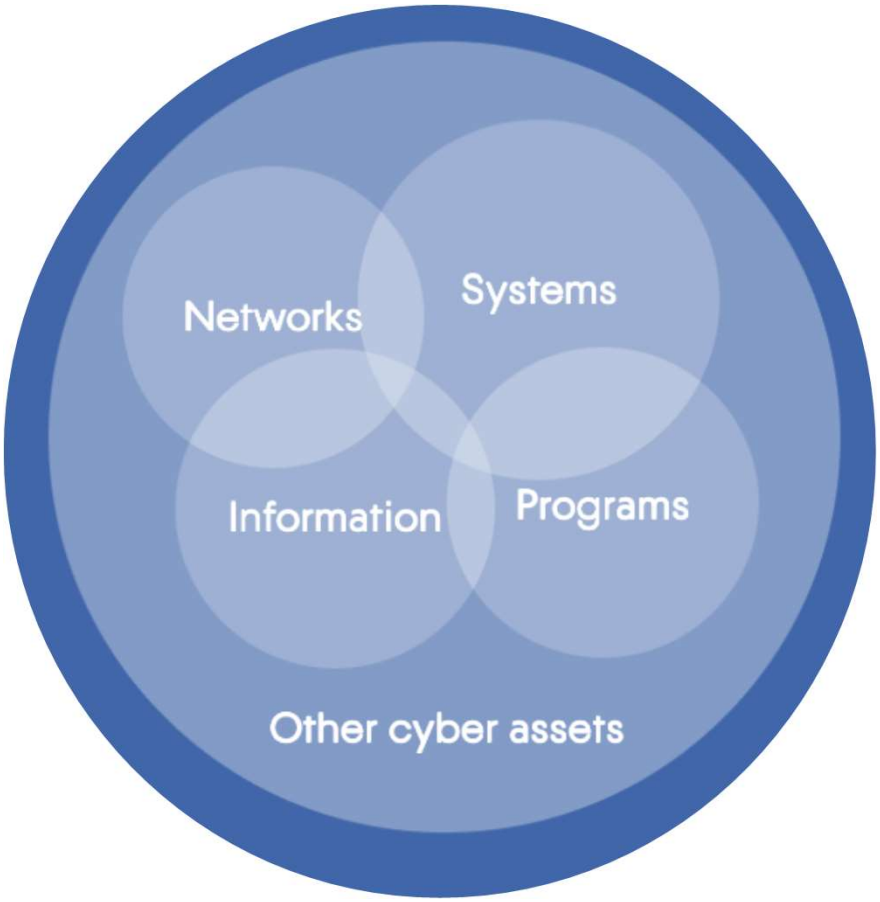
Phishing scams are one of the most common ways hackers gain access to sensitive or confidential information. Phishing involves sending fraudulent emails that appear to be from a reputable company, with the goal of deceiving recipients into either clicking on a malicious link or downloading an infected attachment, usually to steal financial or confidential information.

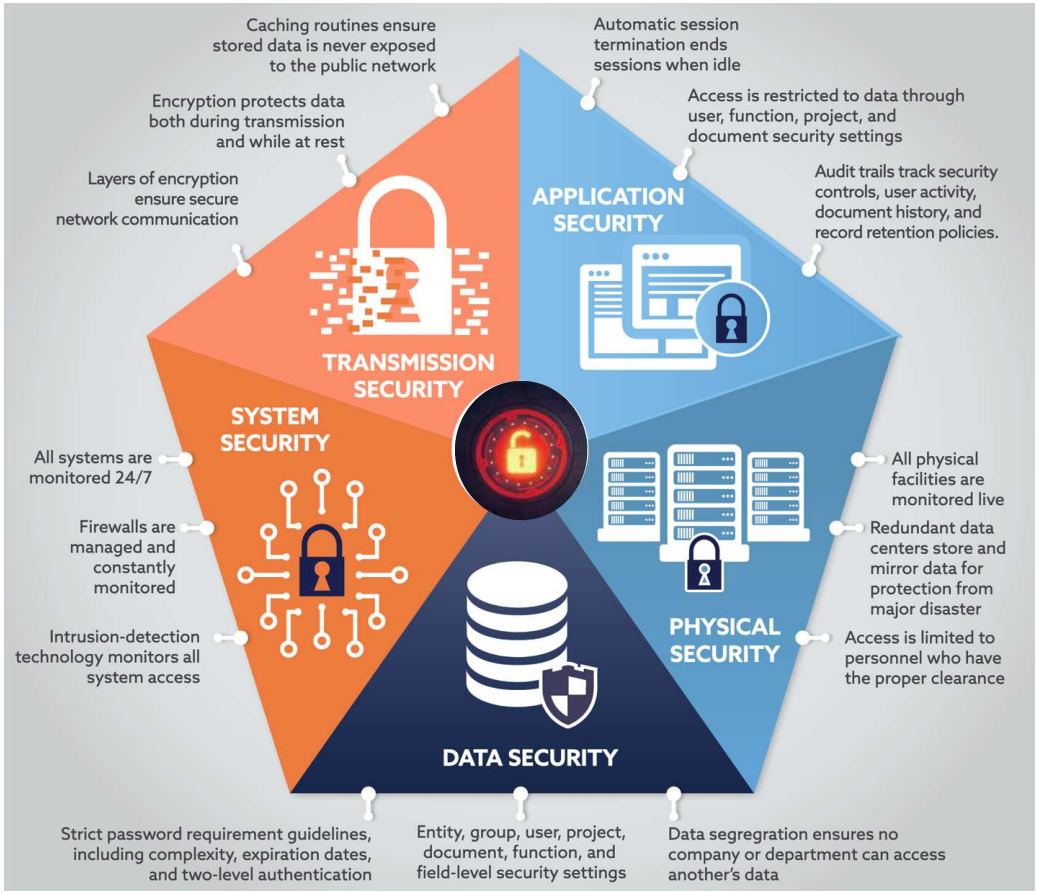
Denial of Service is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. It is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Ransomware is software that gains access to and locks down access to vital data. Files and systems are locked down and a fee is demanded commonly in the form of cryptocurrency.

Community College of Philadelphia
www.ccp.edu

Types of Security





Community College of Philadelphia
www.ccp.edu

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Best Practices from the President's Executive Order

May 12, 2021

- MFA (Multi-Factor Authentication - because passwords alone are routinely compromised)
- Endpoint Detection & Response (to hunt for malicious activity on a network and block it)
- Encryption (so if data is stolen, it is unusable)
- Empowered Security Team (to patch rapidly, and share and incorporate threat information in your defenses)
- Backup your data, system images, and configurations, regularly test them, and keep the backups offline
- Update and patch systems promptly
- Test your incident response plan
- Check Your Security Team's Work
- Segment your networks

Community College of Philadelphia
www.ccp.edu

Data Security Applications & Tools at CCP

Data Security Applications & Tools	Name	Implemented
Malware	Microsoft Exchange Online Protection (EOP) - O365	Yes
Phishing	Microsoft Exchange Online Protection (EOP) - O365	Yes
Virus Protection	Microsoft Exchange Online Protection (EOP) - O365	Yes
Spam	Microsoft Exchange Online Protection (EOP) - O365	Yes
DDoS (Distributed Denial of Service Attacks)	Kinber (Keystone Initiative for Network Based Education & Research)	Yes
MFA (Multi-Factor Authentication)	Unifyed (Partial Implementation)	Yes
Firewall	Fortinet	Yes
NAC (Network Access Control)	Fortinet (Purchased – Implementation started – to be completed by 3/22)	In Progress
Single Signon	Unifyed	Yes
Network Monitoring	Whatsup Gold (Availability) & ForeSite (Log Alerting)	Yes
SIEM (Security Incident Event Management)	ForeSite	Yes
File Transfer Protocol	SFTP	Yes
Encryption	SSL Communications with websites	Yes
DLP (Data Loss Prevention)	Microsoft 365 Compliance	In Progress
Wireless Security	Cisco (Use of ACL's - access control lists) & ForeSite (Monitoring Logs)	Yes
Intrusion Detection (Network Security & Monitoring)	ForeSite	Yes
OS Patching for workstations - PC's	SCCM (Microsoft System Configuration Manager)	Yes
OS Patching for workstations - Apple Mac's	JAMF	Yes
Endpoint Security of Workstations	Microsoft Defender	Yes
VPN Software	FortiClient	Yes
Web Filtering	FortiGate Firewalls and Proxy Servers	Yes

Community College of Philadelphia
www.ccp.edu

Chubb Cyber Insurance Policy

New Program Structure

7/1/2021 – 7/1/2022

CHUBB
$3M LIMIT
Previous Premium: $15,880
New Premium: $28,376

Retention:
$50,000

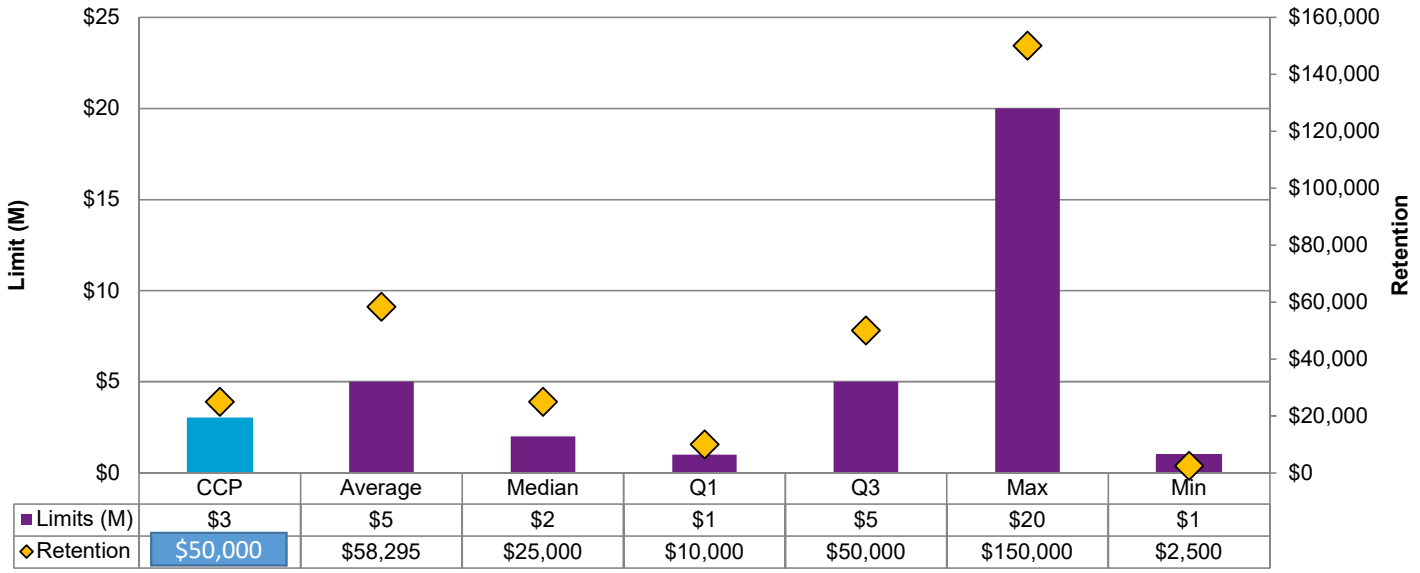
Insuring Agreement	Limit ($)
Third Party Coverage	
Security & Privacy Liability; Regulatory Fines; PCI Fines; Media Liability	$3,000,000
Breach Response Coverage: Notification/Credit Monitoring; Forensic Investigation; PR/Crisis Management; Legal Expense	$3,000,000
First Party Coverage	
Network Business Interruption (NBI)	$3,000,000
NBI due to System Failure	$3,000,000
Dependent Business Interruption (DBI)	$3,000,000
DBI due to System Failure	$3,000,000
Waiting Period	24 Hours
Data Restoration Cyber Extortion	$3,000,000
Reputational Harm	$3,000,000
Hardware Replacement	$3,000,000
Fraudulent Instruction	$100,000

Community College of Philadelphia
www.ccp.edu

Benchmarking

Cyber

Industry:	Education	**Limit:**	CCP's limit is slightly above the median but below the average of its revenue peer group.
Revenue:	Under $100M		
Peer Count:	22	**Retention:**	At $50k, the retention is average relative to CCP's revenue peer group



	CCP	Average	Median	Q1	Q3	Max	Min
Limits (M)	$3	$5	$2	$1	$5	$20	$1
Retention	$50,000	$58,295	$25,000	$10,000	$50,000	$150,000	$2,500

Community College of Philadelphia
www.ccp.edu

Cyber Coverage Overview

- **Breach Response coverages**: Direct breach response costs may include those incurred to hire a law firm, complete a forensic investigation, hire a public relations firm, send notifications to affected individuals, set up call center services, complete identity theft restoration, conduct data reconstruction, and provide credit monitoring services.
- **Network Security and Privacy Liability coverage:** Coverage for indemnity and defense costs for third party claims and regulatory actions alleging a security failure or privacy event. This insuring agreement usually includes coverage for PCI fines, expenses, and costs.
- **Media Liability:** Coverage for indemnity and defense costs for third party claims alleging media wrongful acts such as defamation, disparagement, and copyright / trademark infringement in the dissemination of internet content and media.
- **Business / Network Interruption:** Indemnification for loss of income, incurred extra expenses, and claims preparation costs that arise directly out of a network security breach which disables the insured's network.
- **Contingent Business / Network Interruption:** Extends the business interruption to cover your lost income and extra expenses incurred due to a network interruption occurring at one of your critical third parties or outsourced providers that you rely on to conduct business. Examples of these third parties include cloud service providers, web hosting, and Software as a Service (Saas) providers.
- **System Failure:** Broadens out the business interruption coverage to include interruption resulting from an unintentional and unplanned interruption of the insured organization's computer systems. This includes things like software programming or patching errors that unintentionally bring down the network, hardware or software glitches, and human error.
- **Contingent System Failure:** Extends the System Failure coverage to cover your lost income and extra expense incurred due to a System Failure event occurring at one of your critical third party parties or outsourced providers that you rely on to conduct business.
- **Cyber Extortion:** Covers extortion payments and associated expenses to investigate a security threat to release or refuse to unencrypt sensitive information or to bring down a network unless a ransom is paid. Coverage extends to those payments made via traditional currencies, as well as non-traditional crypto-currencies such as Bitcoin.

Community College of Philadelphia
www.ccp.edu

Cyber Liability

February 2021 update

State of the market and claims, legal, emerging trends

Rate prediction: +25% to >50%

- Cybercriminals are targeting businesses of all kinds with ransomware attacks. As these attacks become more sophisticated, carrying the potential to affect a wholesale inability to access a firm's entire electronic infrastructure, ransom demands have increased — often reaching **eight figures.**
- The SolarWinds cyber event has also given many markets pause.
- This explosion in severity, coupled with high frequency, has had a direct impact on premiums, capacity and underwriting scrutiny.
- Certain carriers have put in place SolarWinds exclusions and are requiring supplemental ransomware applications, even when in an excess position.
- Carriers are starting to sublimit ransomware coverage, 50% of the limit or a 50% co-insurance.
- Carriers are rethinking positions in large towers and looking more closely at rates in perceived burn layers.
- The average cost of a data breach in 2020 was **$3.86M,** according to a new report from IBM and the Ponemon Institute.
- Costs remain highest in the U.S., where the average cost of a data breach was $8.19M, up 5.3% since 2019, driven by a complex regulatory landscape that can vary from state to state, especially when it comes breach notification. Health care was again the most expensive industry, with data breach costs in **2019 averaging $7.13M.**
- The human element continues to be the leading cause of cyber loss, contributing to 62% of the claims included in the 2020 Reported Claims Index.
- According to Willis Re's 4th annual cyber survey of cyber insurance buyers and underwriters, risk managers, claim staff, actuaries and brokers, 86% think the frequency of cyber attacks will in crease as a result of COVID-19 and **over half (54%) think the severity of those attacks will also increase.**

Community College of Philadelphia
www.ccp.edu

Technical Controls & Core Focus Areas

REMOTE DESKTOP PROTOCOL

RDP is a dominant attack vector for ransomware. Recommendations to secure RDP include:

- VPN
- Encryption
- RDP Gateway
- Complex Passwords
- Multi-Factor Authentication
- Restrict access via a firewall
- Enable Restricted Admin Mode

ADDITIONAL SAFEGUARDS INCLUDE

- Placement Within the Network
- Network Level Authentication (NLA)
- Limit Domain Administrator Account Access
- Regular cybersecurity awareness & phishing training
- If using O365, O365 Advanced Threat Protection add-on
- Minimize the number of Local Administrator Accounts & ensure each is unique
- Use of account-naming convention that does not reveal organizational information

MULTIFACTOR AUTHENTICATION

In addition to securing RDP, insurers are looking for insureds to utilize MFA to secure:

- Email
- Network Access
- Privileged User Accounts
- Virtual Desktop Instances (VDI)
- Cloud resources including Office365

BACK-UP POLICIES

Property secured back-ups reduce the severity of Ransomware losses. Recommendations include:

- Encrypting backups
- Segregating backups; physically stored offsite and offline
- Regular testing backups for data integrity and restorability
- Regularly performing full and incremental backups of data
- Annual testing of Incident Response/ Business Continuity Plan