WORK SESSION MINUTES – WEDNESDAY, APRIL 21, 2021

STATE OF KANSAS)
) SS
CITY OF KANSAS CITY)

The Board of Public Utilities of Kansas City, Kansas (aka BPU, We, Us, Our) met remotely in Work Session on Wednesday, April 21, 2021 at 5:00 P.M. The following Board Members were on the teleconference: Robert L. Milan, President; Mary Gonzales, Vice President; Rose Mulvany Henry, Secretary; Jeff Bryant, Thomas Groneman, and Ryan Eidson.

Also on teleconference: William Johnson, General Manager; Angela Lawson, Deputy Chief Counsel; Lori Austin, Chief Financial Officer/Chief Administrative Officer; Jeremy Ash, Executive Director Electric Operations; Steve Green, Executive Director Water Operations; Johnetta Hinson, Executive Director Customer Service; Dong Quach, Executive Director Electric Production; Jerry Sullivan, Chief Information Officer; Jerry Ohmes, Executive Director Electric Supply; Robert Kamp, IT Project Manager; and Dennis Dumovich, Director Human Resources.

A tape of this meeting is on file at the Board of Public Utilities.

Mr. Milan called the meeting to order at 5:00 P.M.

Roll call was taken, and all Board Members were present.

Item #3 – Approval of Agenda

A motion was made to approve the Agenda by, Mr. Groneman, seconded by Ms. Gonzales and unanimously carried.

Item #4 – Board Updates / GM Updates

Mr. William Johnson, General Manager gave the Board an update on the KDHE Loan process. The Unified Government gave their approval to proceed with the loan process on April 8th.

In an update regarding the upcoming APPA National Conference, Mr. Johnson said that no one on the Board wanted to attend the "in person" conference. He had reached out to APPA staff regarding the possibility of organizing an on-line workshop about board governance.

WORK SESSION MINUTES – WEDNESDAY, APRIL 21, 2021

STATE OF KANSAS)
) SS
CITY OF KANSAS CITY)

Item #5 –IT Update

Mr. Jerry Sullivan, Chief Information Officer, gave a PowerPoint presentation to give an overview to the Board regarding the utility's comprehensive approach to Cyber Security to minimize and resolve potential threats as well as the goals to implement Disaster Recovery and Continuity plans. (see attached)

Mr. Johnson commented on system reliability and its connection with vegetation management. It was now a requirement to track and report our numbers to the federal government. Making sure that system reliability wasn't an issue, directly affected economic development. He commended them on doing an excellent job in getting our numbers where they needed to be.

Mr. Sullivan addressed questions and comments from Mr. Johnson and the Board.

Item #6 – Adjourn

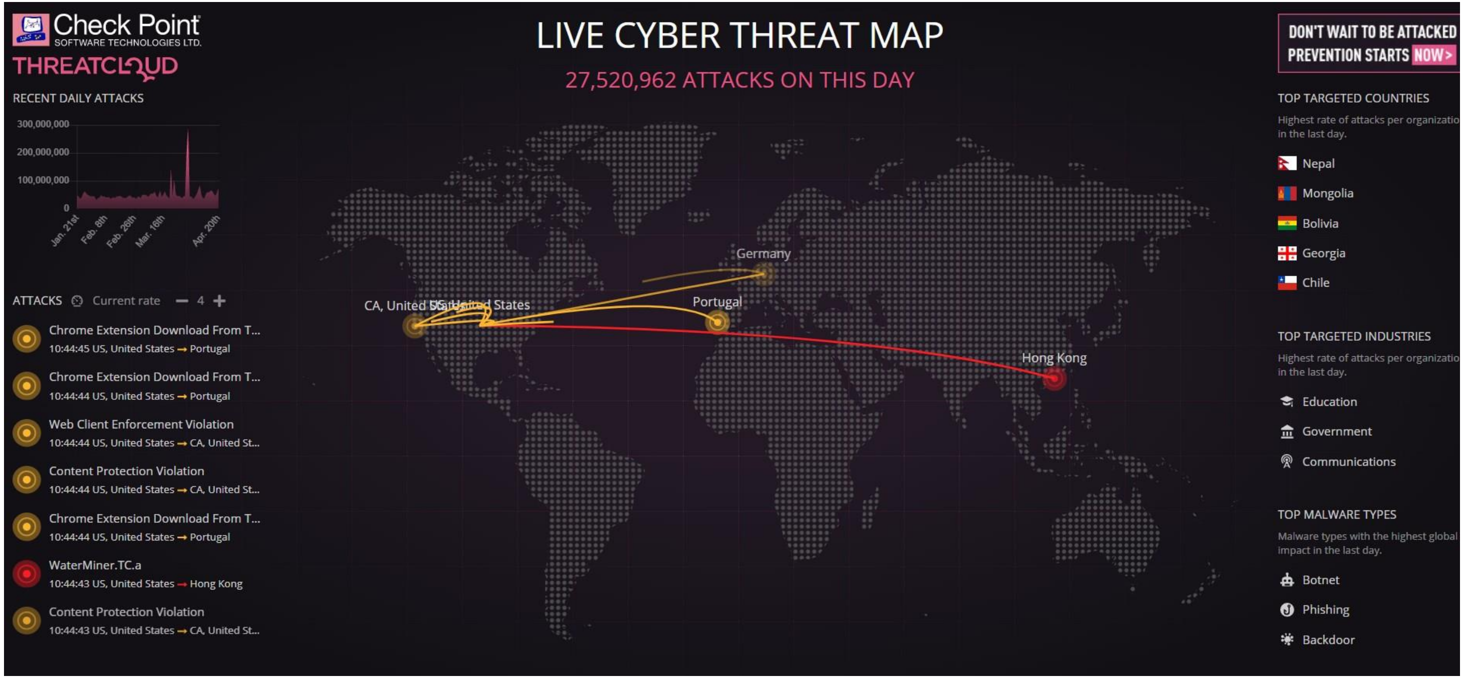
A motion was made to adjourn the Work Session at 5:52 P.M. by Mr. Bryant, seconded by Mr. Groneman and carried unanimously.

ATTEST:
DocuSigned by:
Rose Mulvany Henry
732C225A5806456...
Secretary

APPROVED:
Robert Milan Sr.
President

Live Cyber Threat Map

https://threatmap.checkpoint.com/



Check Point SOFTWARE TECHNOLOGIES LTD.

THREATCLOUD

LIVE CYBER THREAT MAP

27,520,962 ATTACKS ON THIS DAY

DON'T WAIT TO BE ATTACKED PREVENTION STARTS NOW>

RECENT DAILY ATTACKS

ATTACKS Current rate — 4 +

- Chrome Extension Download From T...
  10:44:45 US, United States → Portugal
- Chrome Extension Download From T...
  10:44:44 US, United States → Portugal
- Web Client Enforcement Violation
  10:44:44 US, United States → CA, United St...
- Content Protection Violation
  10:44:44 US, United States → CA, United St...
- Chrome Extension Download From T...
  10:44:44 US, United States → Portugal
- WaterMiner.TC.a
  10:44:43 US, United States → Hong Kong
- Content Protection Violation
  10:44:43 US, United States → CA, United St...

TOP TARGETED COUNTRIES

Highest rate of attacks per organizatio in the last day.

- Nepal
- Mongolia
- Bolivia
- Georgia
- Chile

TOP TARGETED INDUSTRIES

Highest rate of attacks per organizatio in the last day.

- Education
- Government
- Communications

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Botnet
- Phishing
- Backdoor

KANSAS CITY BPU

THE POWER OF COMMUNITY

Cyber Security & Disaster Recovery

April 21, 2021

Cyber / Disaster Recovery Discussion

1. Cyber Security
   a. Threats
   b. Mitigations
   c. Assessments

2. Disaster Recovery
   a. Importance
   b. Threats and Goals
   c. Projects

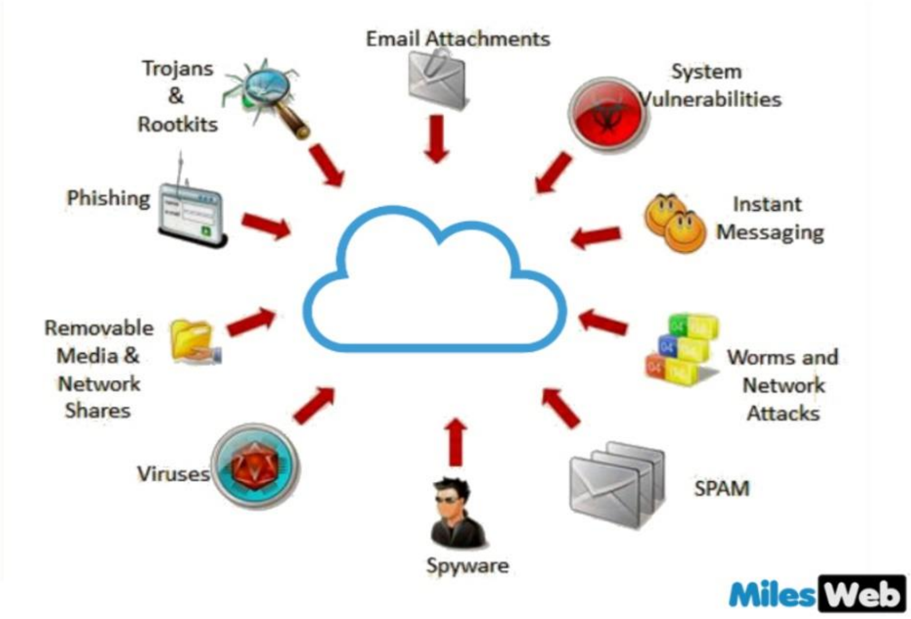
For security; we will not cover specific cyber security details, tools, or protections – if needed it can *be discussed at a secure, Closed Board Meeting*

Cyber Security
Threats

Cyber Security

Utilities are faced with mounting ***threats***. Here are a few:

1. Social Engineering
2. Ransomware
3. DDoS Attacks
4. Third Party Software
5. Cloud Computing Vulnerabilities



Utility CIOs rate Cyber Security as the #1 threat

Cyber Security issues:

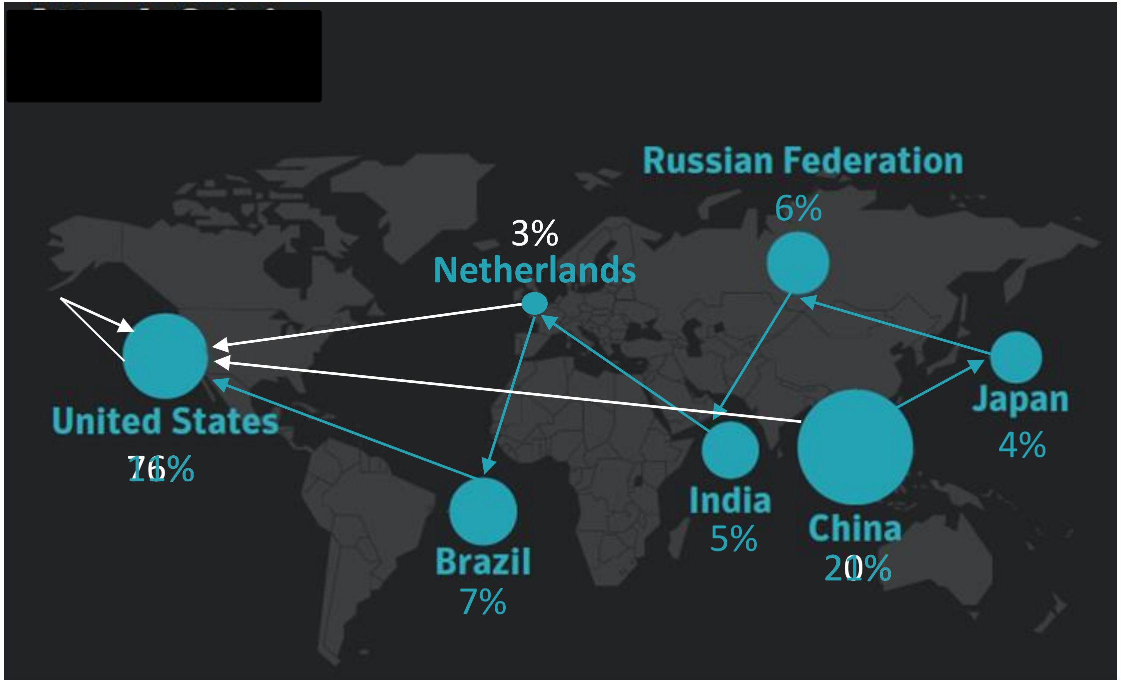
1. Are real
2. Well funded by cyber organizations
3. Happen every day
4. Are increasing in complexity

Therefore, BPU has taken a comprehensive approach to Cyber Security to prevent, minimize, and resolve potential threats --- more on this later.

If it were one threat,
it would be easy.

Initiator Countries Against the U.S.

[redacted]



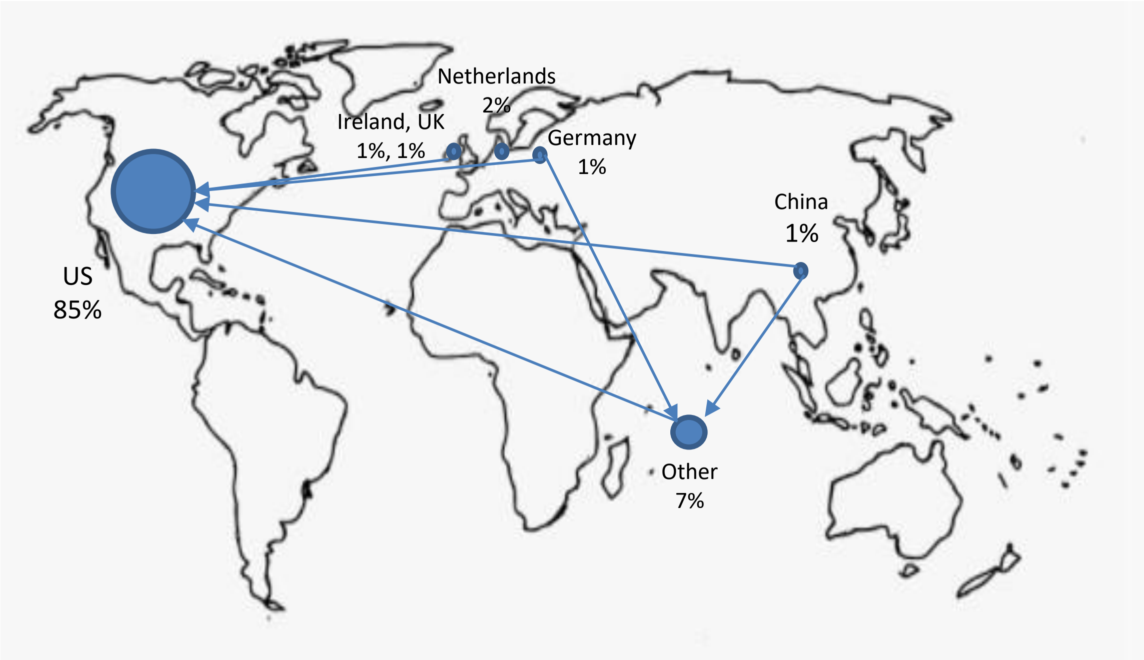
1. For most of the last 7 years, China has been the energy sector's biggest external threat.

2. Russian probes into the US energy sector's firewalls are decreasing.

3. Most utilities now block internet addresses from China, Russia and others, however this practice is becoming less effective.

Source: Symantec, 2018 Internet Security Threat Report, Volume 23, March 2018

Current locations of initiated threats against BPU



1. To reduce numbers of attacks we block known IP addresses from many foreign countries.

2. This measure is less effective now since servers in the US are vulnerable. To circumvent blocking of IP addresses, criminals "jump" through other nations' servers.

3. Most cyber traffic now is directed through US based infrastructure.

Cyber Attack Types

1. Phishing Emails – 70%
2. Malware – 10%
3. Man-in-the-Middle (MITM) – 14%
4. SQL Injection* – 5%
5. Distributed Denial-of-Device – 1%

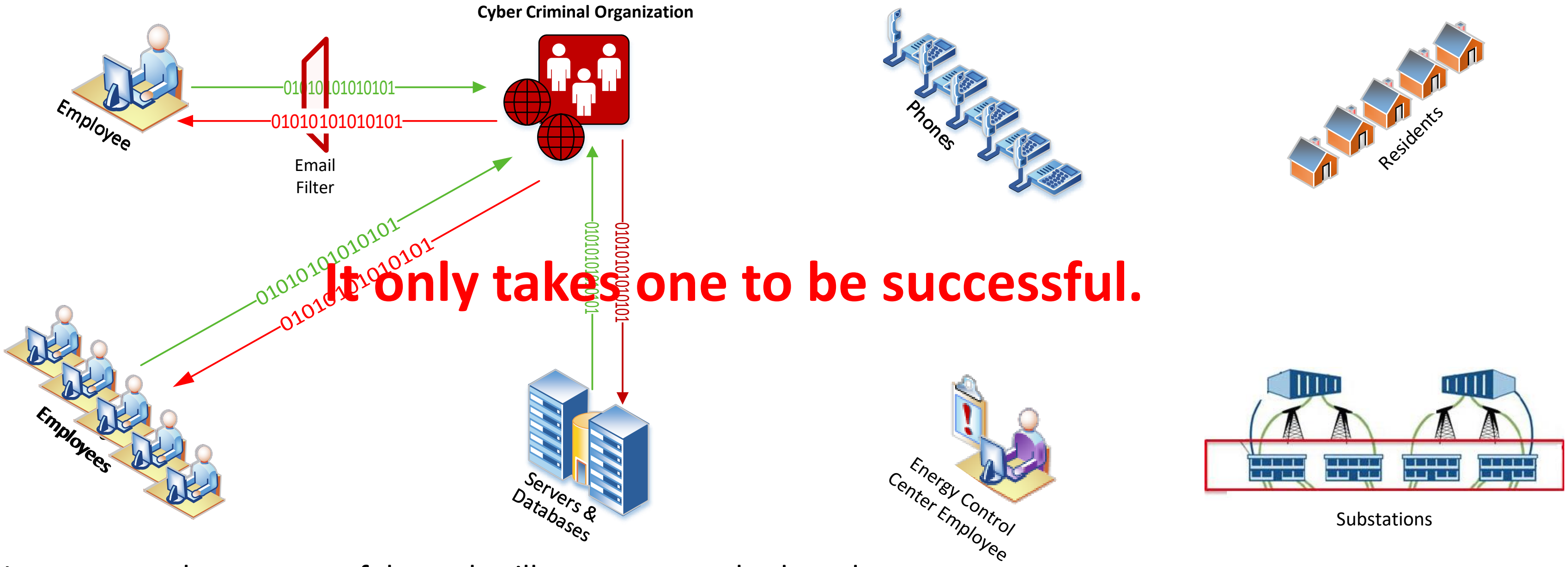
** Although SQL Injection is the least frequent, it is the largest risk.*

Large Public Power Stats 2019

"The usual stuff – a new virus from the Joker, spyware from the Penguin, malicious code from Cat Woman, another phishing scheme from the Riddler."

Example of a critical / coordinated attack on an energy system

The first known successful cyberattack on a power grid occurred on December 2015 in the Ukraine. It was a multi-factor (vector) attack with many underlying exploitations.

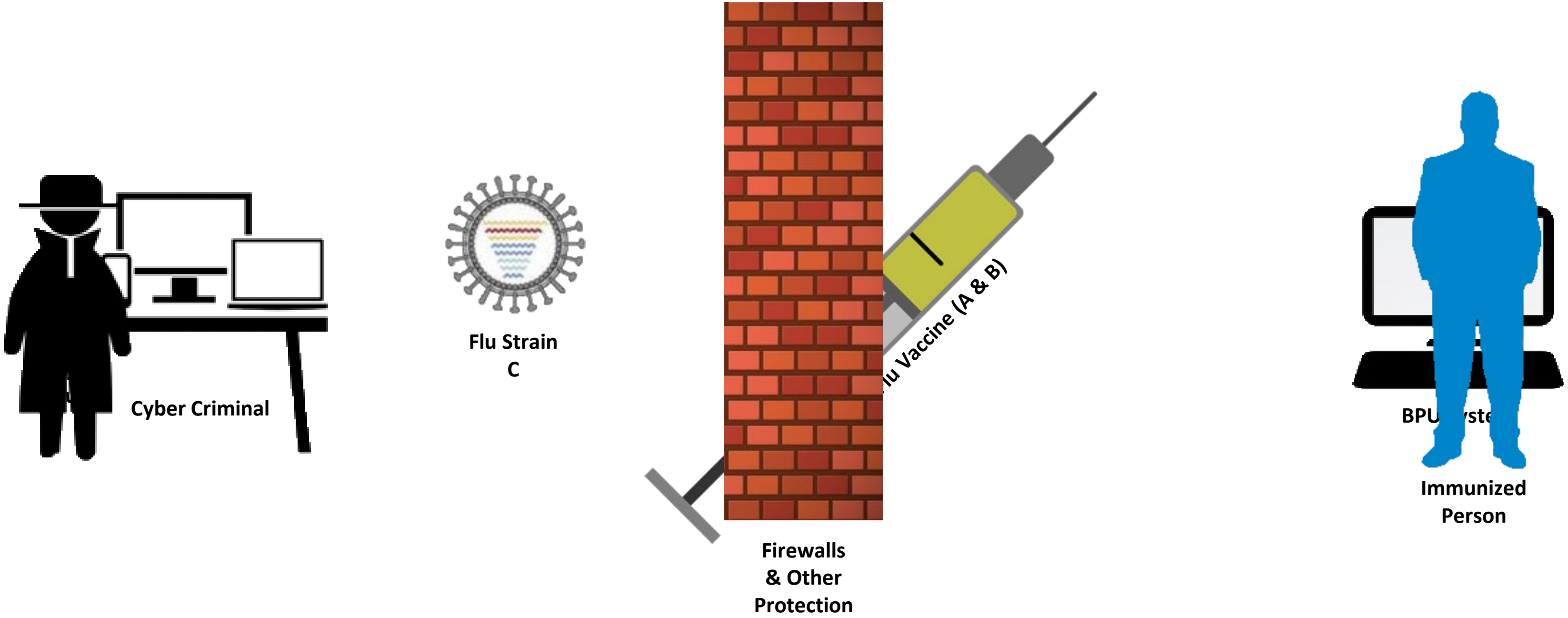


It only takes one to be successful.

BPU can expect that a successful attack will use many methods and vectors.

Mitigation

Firewalls prevent most attack types



BPU’s 2021 Cyber Assessments

- Assessments are planned, budgeted, and conducted throughout the year
- We contract security professionals with the latest tools, and experience
- Recent Cyber Assessments:
  - Penetration Tests
  - External Internet Facing Transactions (Cloud / Web)
  - External Auditor Review
  - Phishing Tests (Rubin Brown and BPU)
  - Monthly Network Security Scanning

KANSAS CITY BPU
THE POWER OF COMMUNITY

Disaster Recovery

Why is Disaster Recovery (DR) important?

- From 2015-2019, more than 50% of companies experienced a downtime event lasting longer than a full workday
- 96% of companies survive ransomware attacks if they have an effective backup and recovery plan
- 93% of companies without DR capabilities are out of business within one year of a major data disaster

---

- Independence Power & Light ransomware attack – Dec 2020
  - Disruption to multiple services
  - Some accounts had up to a 72 day billing cycle
  - Unable to bill accurately for 2 months
  - Absorbed $750,000 in credit card fees

Threats and our Goals

Threats to our technology infrastructure

- Data Center outage
- Acts of nature, e.g. tornadoes, flooding
- Cyber related events
- Criminal activity, physical damage, etc.

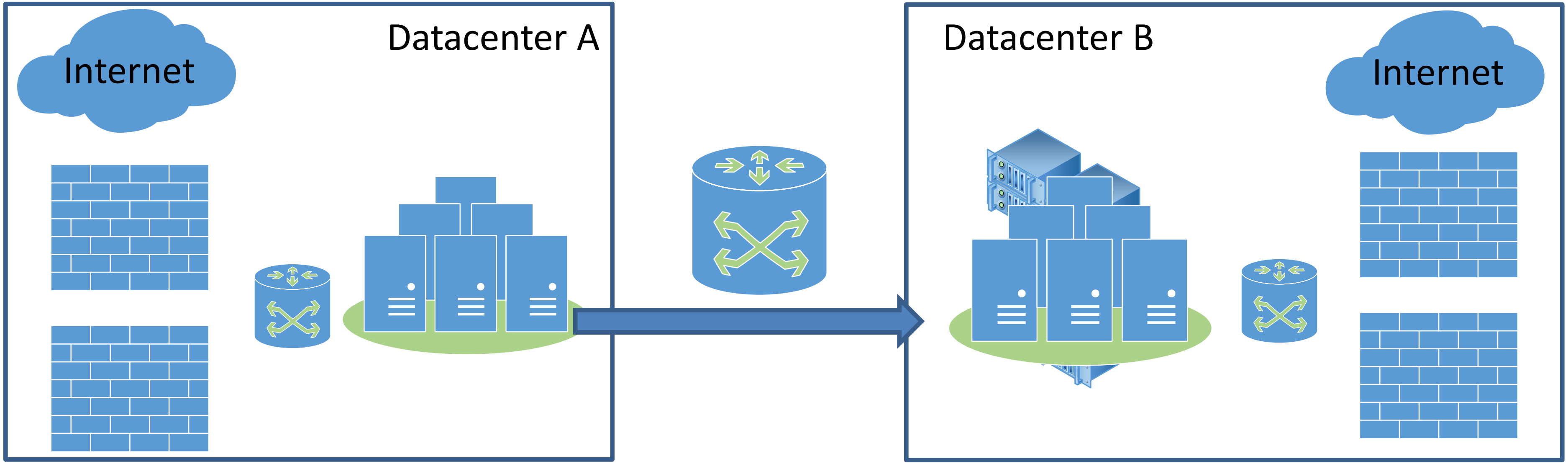
Our Goals

- Implement Disaster Recovery and Business Continuity Plans
- Create Resiliency
- Develop Data Center Redundancy

Utilities need to ***hope*** for the best, but ***plan*** for the worst.

Resiliency/Redundancy of Data Centers

Our process will strive to ensure IT services at an alternate site following a disruption.



Disaster Recovery

2021 Projects

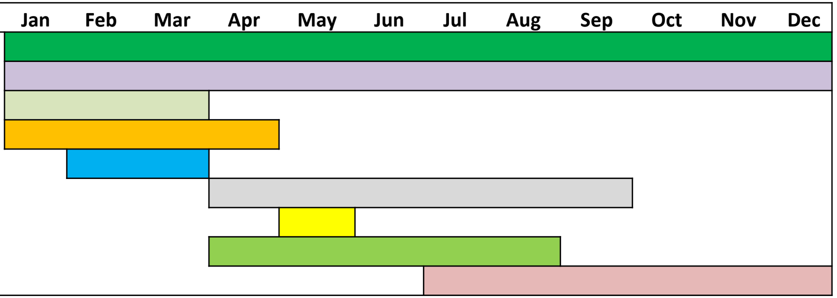
- Disaster Recovery Program
  1. Redundancy and recovery plans for both data centers
  2. Upgraded software
  3. New Hardware (servers and storage)
  4. New processes
  5. Built-in redundancy
  6. Possibly a third data center in hybrid cloud

Resiliency

Disaster Recovery
Project Plans

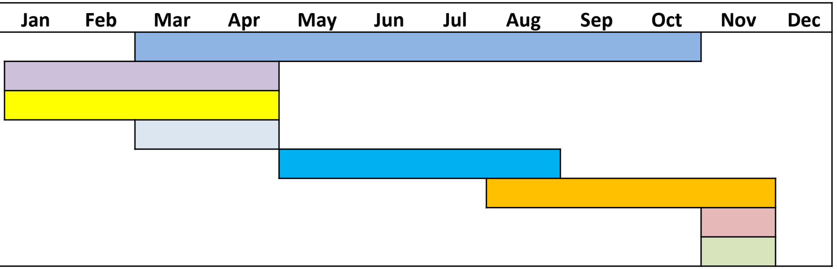
Cyber Security

Name	Start	Finish	Deliverables
Security Awareness Training	01/01/21	12/31/21	Ongoing training
Monthly Security Scanning	01/01/21	12/31/21	Idenitified vulnerabilities
Virus scan upgrade	12/01/20	03/31/21	Current & supported software
Network Security Assessments	01/01/21	04/28/21	Idenitified vulnerabilities
Security Risk Assesment platform	02/01/21	04/01/21	Cyber security risk analysis
Consolidated email & URL filtering	04/05/21	09/06/21	Streamlined administration
Firewall replacement - 2 devices	05/03/21	04/09/21	Current & supported firewalls
IT Security Operations Center	05/03/21	11/14/21	Managed Security Operations Center
IPS/IDS End of Life	07/12/21	01/13/22	Current & supported IPS/IDS appliance



Disaster Recovery

Name	Start	Finish	Deliverables
DR Site Build Out	04/05/21	10/22/21	Servers, storage, network, security equip
VMware farm load balanced	01/18/21	04/30/21	50/50 production split between DCs
DB & VMware server capacity	01/11/21	01/31/22	Added servers for DR site
Assessment phase	03/15/21	04/09/21	State of the program
Documentation phase	04/12/21	08/13/21	Updated templates and plans
Exercise Recovery Plans	08/16/21	11/05/21	Test planning and test completion
Conduct final assessment	11/08/21	11/12/21	State of the program
Program wrap up	11/15/21	11/23/21	Updated documentation and plans



Questions?