www.hometownconnections.com
12081 W. Alameda Parkway, # 464
Lakewood, CO 80228
P — 970 682 4217

Hometown Connections

June 2021

Cybersecurity After COVID-19: 10 Ways To Protect Your Utility & Refocus On Resilience

In the wake of the COVID-19 pandemic and the resultant implementation of social distancing directives, altered business processes, and new economic realities, community-owned utilities must review and address their technology infrastructure and cybersecurity measures.

The swift changes brought about by COVID-19 — including the movement of a large portion of the workforce to telework and the expansion of e-commerce footprints — has caused many organizations to implement new IT capabilities ad hoc. Some provisional solutions have bypassed normal development, approval, and deployment processes, which have often stretched or violated existing cybersecurity policies at the same time that the activity of bad actors has increased globally.

Preparing For The Post-Pandemic World

As social distancing measures abate, organizations will need to de-risk the enterprise and adapt operations to a "new normal." This will require a thorough evaluation of pandemic-driven IT and cybersecurity changes, some of which were rapidly put in place during the response phase of the pandemic, followed by strategic adjustments of enterprise architectures, cybersecurity controls, and business processes based on long-term operating strategies.

Even during "normal" times, policy often lags behind reality in today's IT enterprises. In the pandemic rebuilding period, policy and documentation will need to catch up. Some changes made to address the pandemic may need to be institutionalized; others may need to be replaced with more secure and permanent solutions. All changes should be viewed through a resilience lens, leading to a more agile and secure future for businesses.

As societies recover from pandemic-fighting postures, we can anticipate some features of the post-COVID-19 business world, including:

- Increased and institutionalized remote working.
- Accelerated migration to cloud infrastructure and applications.
- Growth in functionality and use of online collaborative tools.
- A rise in e-commerce.
- Expanded cyber-attack surfaces due to increased telework.
- More attention to enterprise resilience.

In the post-COVID-19 world, these 10 areas will require attention.

1. Teleworking Solutions

Anticipating a permanent increase in telework, community-owned utilities , as well as their public power joint action agencies and state/regional associations, should consider:

- Procuring sufficient on-demand bandwidth to move content, especially video teleconferencing, across and between geographically dispersed sites.
- Establishing VPN capacity through deployment of Internet Protocol Security (IPsec)-based VPN clients or other secure connectivity solutions to employee workstations.
- Managing identity and access for a remote workforce that meets corporate security requirements and employees' ease-of-use needs.
- Implementing mobile device management solutions to address the use of company-issued and approved personal mobile devices for business purposes. In coordination, consider implementing adequate bring-your-own-device (BYOD) policies, such as those outlined below.
- Closely examining enterprise use of internet-based remote desktop protocol (RDP), which allows remote access of Windows systems and servers and is an enticing target for hackers. If its use is justified, companies should consider allowing RDP only with network-level authentication of the endpoint and rigorous patching, including the BlueKeep vulnerability on all Windows machines.

2. External Perimeter Protection

A rise in remote connections can increase a company's cyber-attack surface. Organizations may protect their external perimeters by:

- Implementing network access control (NAC) to authenticate and validate devices and enforce security policies before permitting them to connect to corporate in-office or remote networks.
- Locking down user workstations and company-issued laptops with a defined security configuration, managing configuration centrally, and not assigning administrative privileges to end-users.
- Implementing remote endpoint isolation and forensic capabilities that meet forensic chain-of-custody requirements.
- Implementing capabilities that support remote endpoint data collection and analysis to identify unauthorized activity.

3. Cloud Services

Cloud services can offer significant cost, efficiency, resilience, and potential security benefits over data storage and application hosting alternatives. But these benefits require cloud services to be deliberately and strategically adopted and managed. Companies should consider:

- Adopting formal strategies for the use of cloud services.
- Developing complete inventories of current cloud usage in the enterprise, and rationalizing the use of multiple services.
- Defining data storage policies outlining the conditions required for the use of cloud services, data center storage, and local storage, particularly for sensitive information.

A cloud access security broker is an on-premises or cloud-based software that monitors cloud activity and enforces security policies. It can help detect and monitor cloud usage within the enterprise, enforce related cybersecurity policies, alert administrators of anomalous data flow, and guard against malware.

4. Secure Collaboration Tools

While email, office productivity tools, and video conferencing have been vital during the pandemic, utilities may choose to innovate by adopting and using additional secure collaboration tools. Organizations should explore emerging capabilities, such as augmented/virtual reality or chatbots for content delivery, which can enhance their operations.

5. Cybersecurity Policy

Refresh cybersecurity policies to address pandemic-triggered IT capabilities, architecture, and processes. Organizations should consider conducting a risk assessment and identifying enforcement mechanisms, such as multi-factor authentication, single sign-on, and automatic logout from unattended devices.

6. BYOD Policy

Many organizations chose to allow employees to use their personal devices, including laptops, mobile phones, and tablets, for company business during the pandemic, even though some had prohibitions in place prior to the emergency. Business phone calls were routed to personal mobile phones, email was made available on personal devices, and employees were permitted to access cloud-based applications from personal devices. Organizations should establish a policy, examine or reshape it, and properly document any measures implemented during the pandemic.

7. Cyber Incident Breach Response (CIBR) Plan

Community-owned utilities with strong and current CIBR plans should consider incorporating lessons from the contingency operations brought about by the pandemic. If there was no pre-existing CIBR plan, the need for one should be apparent. Utilities may:

- Refresh and update CIBR and disaster recovery plans to address the current operational context.
- Coordinate and cross-reference CIBR plans with disaster recovery, business continuity, and enterprise crisis management plans to create comprehensive crisis planning document sets.
- Maintain these documents as regularly exercised living plans.

8. Supply Chain and Third-Party Management

The pandemic may have led your supply chain partners and other third parties to transform their business models. Utilities should consider:

- Reviewing third-party agreements, including service-level agreements with IT providers, to ensure they meet current requirements and have acceptable liability provisions.
- Conducting cybersecurity audits and establish ongoing audit requirements for all third parties with authorized access to company networks, systems, or data.

9. Cyber-Attack Financial Protection and Recovery

Changes to your IT infrastructure, from new physical assets to cybersecurity measures, should be accounted for in your cyber risk profile, with adjustments made to insurance coverages as needed. As cyber risk is not solely an operations or technology risk, it is critical to manage both cyber infrastructure and organizational financial exposures. Consideration should be given to cyber insurance, which can provide a cost-effective and critical financial backstop in the wake of a cyber-attack during a pandemic or other significant social and economic crisis. Community-owned utilities should:

- Review existing insurance coverage, including identifying potential gaps.
- Examine how new cybersecurity challenges fit into the organization's cyber risk transfer strategy.
- Be aware of potential changes in coverage terms and conditions at renewal as insurers assess losses and changes in claim patterns post-pandemic.

10. Cyber Operations

The post-pandemic operating environment will be different. Companies should consider:

- Monitoring the central collection and analysis of cybersecurity alerts and audit logs to detect and respond to suspicious/malicious activity.
- Reviewing and updating VPN profiles and firewall rules so employees receive appropriate role-dependent privileges.
- Implementing or refreshing processes for obtaining approval from data and system owners for the provisioning and de-provisioning of remote VPN and other accounts associated with critical business applications.
- Disabling split tunneling for VPN profiles to prevent remote employees from accessing the internet directly from their personal laptops while also accessing corporate information systems.
- Creating a simple mechanism to flag and forward suspicious emails for technical analysis.
- Provisioning secure access solutions with sufficient capacity for the increased numbers of remote users and security protection on endpoints.
- Enforcing software updates to remote workers' company-issued computing devices.
- Enabling multi-factor authentication for VPN and critical information systems.
- Increasing IT help desk capacity and hours of operation to handle a remote workforce's increased service requirements.

A New Focus On Resilience

Today's IT and network capabilities have enabled the strategies that have kept many organizations afloat during the pandemic. The current crisis, however, has highlighted the need to prepare for serious business disruption. A recent survey found that more than a fifth of organizations have shopped for new security solutions or services to respond to their new reality.

Organizations should consider blending new cybersecurity investments with enhanced cyber insurance coverage to reduce their retained risk, optimize spending relative to protection, and conserve resources. The pandemic has illuminated the need for enterprise resilience in stark and compelling terms. The post-pandemic recovery and preparation period presents the opportunity for community-owned utilities to rebuild to a new normal, with enterprise resilience as a pervasive goal.

For More Information & Insights

Ryan Weber
Public Power & Utility Practice
Marsh USA Inc.
Ryan.weber@marsh.com
281-732-1558

Marsh

Hometown Connections | Partner

About Marsh

A partner of Hometown Connections, Inc., Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $17 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to BRINK.

About Hometown Connections, Inc.

Hometown Connections, Inc. is a national, non-profit utility services organization serving community-owned utilities. A single source for many utility products and services, our team of consultants and vendor partners provide affordable and high-quality solutions to help community utilities transform business operations, planning, employee engagement, the customer experience, and much more. Supporting operational and service excellence, all of our services and deliverables are scalable based on the size and objectives of the utility. @HTConnections, Facebook, LinkedIn.