// Are You Prepared For Cyber Blackout?

Advanced Incident Preparedness with Wickr

Fortune favors the prepared. For cyber incident responders and continuity experts, the most critical time to act is *before* an incident occurs.

Increased dependence on electronic communications and IT systems means increased vulnerability to a scenario coming to be known as Cyber Blackout (CBO). In a CBO, operational conditions in the wake of an outage or security incident degrade to the point that critical systems can no longer be used or trusted. The breadth of such an event can have a significant impact, recursively affecting the business and the ability of its response team to investigate and restore operations.

Preparing for CBO starts with an understanding of what's important to you and when. The need for redundancy for systems like web and application servers is long understood and prominent in most organizations' contingency plans. The availability of communication services like internal chat and email, however, is often assumed, and not part of most contingency plans. What if communication services are also targeted in an attack? What if they are compromised? What if you're not sure?

"Given the multitude of attacks and access to communication solutions, enterprises need to deploy, manage and have flexible administrative controls to not only secure sensitive communications, but follow best practices for retaining information as required. Wickr is the only product that offers this through strong encryption, deployment options and selective controls."

- Joe Sullivan, Experienced CSO (Facebook, Uber, Cloudflare), Commissioner on President Obama's cyber commission and former Federal Prosecutor

Secure communications are vital to a response team. Information shared in the course of an incident investigation - including items such as infrastructure scan results, vulnerabilities found, countermeasures in place, investigation summaries, next steps, and the identity of key personnel – is extremely valuable to an attacker in their effort to evade detection and maximize damage while the incident is ongoing and could do great long term harm to your organization if exposed publicly.

support@wickr.com
Wickr® and //® are registered trademarks and Wickr Inc. Copyright © 2018 Wickr Inc

The growing awareness of this threat is increasing investment in contingency planning and informing best practice, which now requires plans and responses for Cyber Blackout scenarios. Proactive organizations have evolving strategies and playbooks built to provide clear direction for each team member during CBO. Crisis communication and IR related documentation will have been created, discussed and updated on a regular basis as part of ongoing readiness and training. Best practice is to ensure there is a reliable out of band channel for these communications and planning.

Out of Band Communications

Highly secure, out-of-band communication channels are deployed, configured and regularly exercised to provide the necessary capabilities in times of crisis. These communications are required to include 1:1 and group messaging with internal and external personnel, audio/video conference calling, file sharing, and API integrations for advanced orchestration and workflows. Usage and data retention policies are promulgated within the secure out of band collaboration platform and enforced with proper tooling. Team members are pre-provisioned into communication systems and organized by function, geography, seniority, and group to ensure seamless functioning in times of crisis. Using modern orchestration tools and techniques the appropriate information, logs and communications are automatically sent to the proper teams in their respective secure Wickr Rooms.

Wickr supports all phases of the incident response process

Wickr® and //® are registered trademarks and Wickr Inc. Copyright © 2018 Wickr Inc

Learning from Prior Incidents

Examples of CBO incidents include Sony, Maersk, and Merck. Much was learned from the Sony breach of 2014, where attackers not only compromised documentation, movies, and personnel information, but also gained access to Sony's internal communication channels. From this vantage point, attackers were able to monitor Sony's IR discussions and response scenarios to the attack, thus thwarting Sony's ongoing efforts, extending the PR story and compounding the overall damage. The primary lesson learned for all industry was that any tool used for communication must be secure and must not depend on existing infrastructure. More recently, organizations like CBS have learned that simply being out-of-band isn't enough – you must use a tool that meets all needs including compliance services that ensure operation in accordance to information governance policies and within regulatory guidelines.

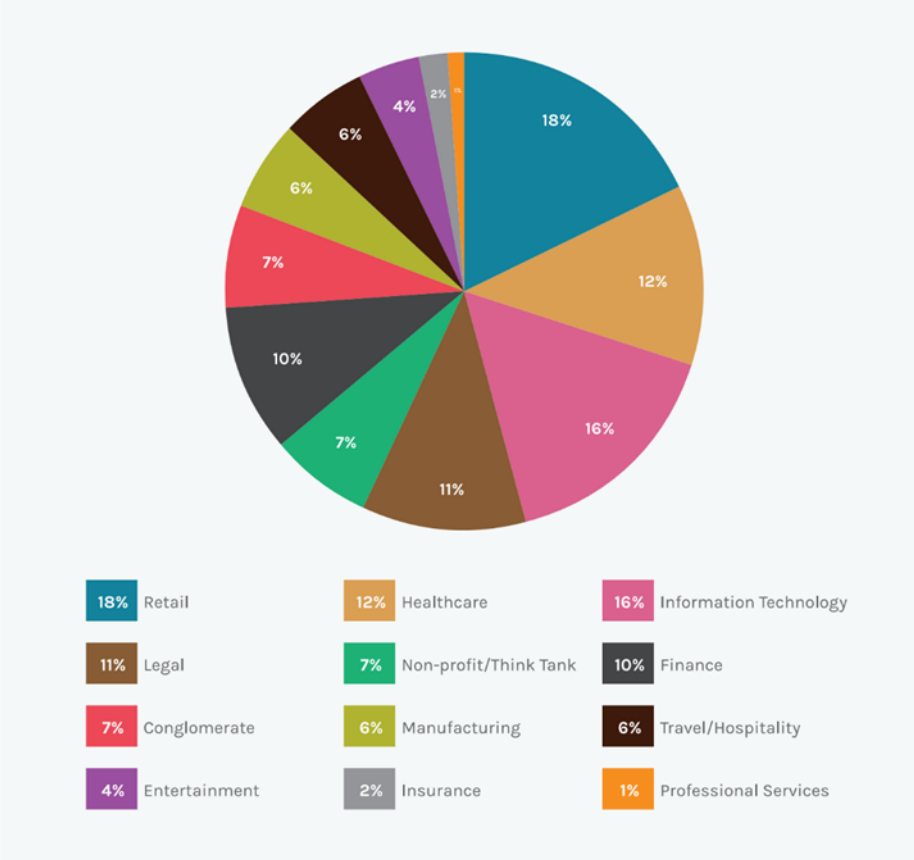

Fig. (1)? Many industries face cyber breaches. Cyber Instrusion Services Casebook (Crowdstrike, 2017), https://www.crowdstrike.com/resources/reports/cyber-intrusion-services-casebook/

Wickr® and //® are registered trademarks and Wickr Inc. Copyright © 2018 Wickr Inc

Wickr Pro – Empowering Response Teams

Proactive organizations use Wickr to improve their cyber crisis readiness and response for CBO and beyond. Wickr Pro empowers response teams with reliable, out-of-band, end-to-end secure messaging, file transfer, voice and video conferencing and screen sharing with no complicated configuration or IT management required. With Wickr Pro, teams can manage crises and maintain readiness through performance of important day-to-day activities such as:

- Daily stand-up calls with the Hunt, IR and Crisis teams to address threats that are detected through ongoing investigations
- Project status meetings to organize teams and to share updated documents and information
- Monthly team calls for secure video conferencing and collaboration
- Periodic information exchange with outside consultants and subject matter experts

Wickr voice and video conferencing also helps you prepare for CBO scenarios that impact traditional on-premises PBX phone systems. Being cloud based, Wickr Pro communications services are globally accessible and available in multiple data centers over IP-based wired, WiFi and mobile data networks, freeing you from the constraints of on-premises hardware that could bottleneck your recovery efforts.

With Wickr, you can ensure the right people are in the right virtual rooms to receive the right information from each other and from internal or external workflow systems, SIEMs and log aggregators via API integration. Strong mobile and desktop device security and default ephemerality ensure that all information has a time to live and won't linger past its useful life to potentially spark future incidents.

Deploying Wickr more broadly in your organization can even help prevent CBO by securing your highest risk communications all day, every day beyond your security team to your executives, legal and strategic staff.

Contact us and see how Wickr Pro provides the broadest feature set and strongest security on the market - for CBO and beyond.

Wickr® and //® are registered trademarks and Wickr Inc. Copyright © 2018 Wickr Inc

Wickr is a turn key software and service solution including:

	Wickr
256-bit End-to End Encryption, FIPS 140-2, NSA Suite B compliant	✓
Perfect Forward Secrecy	✓
Ephemerality by Default	✓
Device to Device (no server-side dependence)	✓
End-to-End Encrypted Group Messaging, Calling, Video Conferencing, Screen Sharing & Audio Memos	✓
Peer to peer Group Management Protocol - Defends against attacks aimed at manipulating group membership	✓
End-to-End Encrypted Large File Sharing (5 GB)	✓
Message Recall - Delete message from both sender and recipient device	✓
Starred Messaging (for easy follow up)	✓
User Verification	✓
Federated messaging for secure communications outside of your network	✓
White Label for Customized UI - Customer may personalize with their brand, logo, etc	✓
Single Sign On - Easy adoption and provisioning - Convenience of onboarding and security of offboarding	✓
Multiple Levels of Ephemerality - 365-day max Time to Live in Wickr Pro and fully customer defined with Wickr Enterprise - Additional Burn on Read capability within Wickr per each message	✓
Enterprise Administrative Controls - Powerful management of users, groups, rooms, auto-provision and de-provision to stay within policy guidelines set by customer - Strong account access control options - Compliance/data retention (Wickr Enterprise)	✓
Integration via Bots and APIs - Extend Wickr to additional workflows in existing customer applications - Implement scenario-based data sharing/reporting with third parties and affiliates	✓
Single-Tenant, Multi-Tenant and Private Cloud Hosted Deployment Options	✓
Wickr® - Open Access Smart VPN for seamless and secure global connectivity	✓
Enterprise Support	✓
iOS, Android, Windows, OS X and Linux Clients	✓

Wickr® and //® are registered trademarks and Wickr Inc. Copyright © 2018 Wickr Inc