GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Crane, Casey

Title: "Data Security: Disaster Recovery Plan"

Website: Hash It Out blog by The SSL Store

Organization: The SSL Store

Date: 17 April 2019

URL: https://www.thesslstore.com/blog/in-case-of-emergency-a-disaster-recovery-plan-checklist-for-data-security/

Accessed: 21 Oct 2019
Synopsis: Hurricane season is around the corner and cyber attacks are ever-increasing — is your business prepared for any incident with a disaster recovery plan?

While it's important to plan for an emergency in terms of IT infrastructure and data security preventative measures, it's equally as important to have a disaster recovery plan (also known as a DR plan or DRP) in place to help your business recover from an emergency. Disasters of any kind — natural and man-made alike — pose significant threats to every business and organization. According to research from Keeper Security, Inc. and the Ponemon Institute, 67% of small businesses experienced a cyber attack in the past 12 months.

In its Global Risks Report 2018, the World Economic Forum (WEF) ranks extreme weather events and natural disasters as the top two most likely global risks, followed immediately by cyber security attacks and data theft.

In Case of Emergency: A Disaster Recovery Plan Checklist for Data Security

April 17, 2019 0

In Case of Emergency: A Disaster Recovery Plan Checklist for Data Security

Hurricane season is around the corner and cyber attacks are ever-increasing —

is your business prepared for any incident with a disaster recovery plan?

While it's important to plan for an emergency in terms of IT infrastructure and data security preventative measures, it's equally as important to have a disaster recovery plan (also known as a DR plan or DRP) in place to help your business recover from an emergency. Disasters of any kind — natural and man-made alike — pose significant threats to every business and organization. According to research from Keeper Security, Inc. and the Ponemon Institute, **67% of small businesses experienced a cyber attack in the past 12 months**.

In its Global Risks Report 2018, the World Economic Forum (WEF) ranks extreme weather events and natural disasters as the top two most likely global risks, followed immediately by cyber security attacks and data theft.

Natural disasters that affect businesses include hurricanes, tornadoes, floods and monsoons (yes, we have them in the Southwestern United States as well), earthquakes, wildfires, and blizzards. Man-made disasters for businesses, on the other hand, include everything from terrorist attacks and IT infrastructure attacks to insider attacks, data theft, and cyber attacks. These lists don't even include other unintentional IT infrastructure threats such as rodents eating through critical wiring, power outages, facility fires, plumbing failures, or a slew of other concerns.

In their 2019 Official Annual Cybercrime Report, Cybersecurity Ventures and the Herjavec Group predict that **cybercrime alone will cost the world more than $6 trillion annually by 2021.** This estimate encompasses costs that include:

> *"…damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm."*

No matter what the cause, IT security failures are a very real and critical concern for any organization that uses and depends on information technology resources and data — which, essentially, includes virtually every organization in the modern era. No matter whether you work for a government organization, a small business, or an international corporation, it's imperative to develop and implement a disaster recovery plan and corresponding processes that will help increase your organization's cyber resilience. After all, when the manure hits the fan, you don't want to find yourself wringing your hands, uncertain about how to get your systems back online and operational. The industry-accepted average cost per minute of downtime is $5,600 — which equates to a staggering **$336,000 per hour** (depending on the size of the organization, it could be even more!). Now is the time to make sure you have an IT disaster recovery plan in place that you can implement at a moment's notice.

What exactly is a DR plan and how do you create one? As we like to say around here…

Let's hash it out.

Table of contents

What is a disaster recovery plan? How does it differ from incident response or business continuity plans?

A DR plan is a document that outlines how you will get your essential IT infrastructure and operations up and running after a man-made, natural, or extreme weather emergency. This differs from an **incident response plan (IRP)**, which helps you respond to a cyber security attack and implement corrective measures to respond to and mitigate the threat, and a **business continuity plan (BCP)**, which aims to get a business back to full operations following an emergency. Disaster recovery and business continuity plans, which are closely related in that a DR plan is part of an overarching BC plan, are integral to the success of your business.

A comprehensive disaster recovery plan will include a variety of information such as:

- Guidelines and checklists for determining DR plan activation, escalation, incident, and rollback procedures;
- Strategies and technical processes to follow for implementing recovery procedures
- Personnel information and disaster recovery roles/responsibilities; and
- Rollback procedures for bringing the organization back to a standard operating state.

What to do before creating a disaster recovery plan

To create an effective disaster recovery plan, it's essential to have a full understanding of the situation by performing a **cyber risk assessment** (CRA) that follows National Institute of Standards and Technology (NIST) guidelines and a **business impact analysis** (BIA).

In business continuity and disaster recovery planning for IT professionals, it's about understanding the risks and consequences of cyber attacks or other disasters to your IT infrastructure and data security. Conducting a cyber risk assessment and a business impact analysis can help you increase your cyber resilience by identifying threats to your data security and their impacts should they become successful. In their fourth annual study on The Cyber Resilient Organization, the Ponemon Institute and IBM Security define cyber resilience as follows:

> *"We define cyber resilience as the alignment of prevention, detection and response capabilities to manage, mitigate and move on from cyberattacks. This refers to an enterprise's capacity to maintain its core purpose and integrity in the face of cyberattacks. A cyber resilient enterprise is one that can prevent, detect, contain and recover from a myriad of serious threats against data, applications and IT infrastructure."*

Since incidents affecting IT security and infrastructure can be more than cyber attacks, we also like the definition from the U.S. Computer Emergency Readiness Team (US-Cert) Critical Infrastructure Cyber Community Voluntary Program's (C³ Voluntary Program) CSR Supplemental Resource Guide on Incident Management:

> *"Cyber resilience is the organization's ability to adapt to risk that affects its core capacities."*

This is where BIAs, in addition to CRAs and DR plans, can be particularly helpful. According to Ready.gov, a business impact analysis "predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies."

As organizations along the coastlines of the United States prepare for the whirlwind of hurricane season, we thought it would be beneficial to provide a disaster recovery plan checklist to help you "cross your 't's and dot your 'i's."

10 critical components for every disaster recovery plan checklist

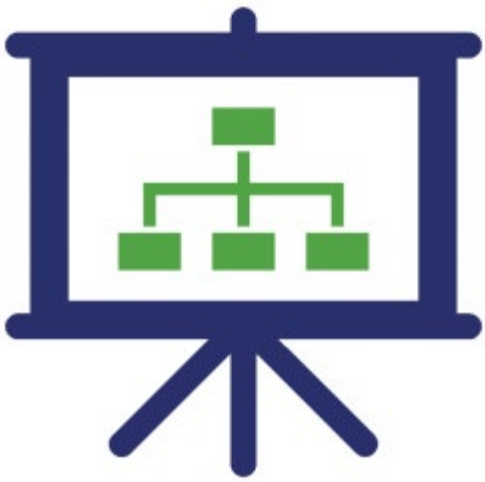
A disaster recovery plan outlines the necessary steps to bring a business back online at the conclusion of an event. Corresponding recovery strategies should be created that account for the potential loss of any vital system components such as hardware, software applications, or data.

In each of the following sections, we'll include examples of information to include or that should be covered in your DR plan. Here are the 10 critical components of our disaster recovery checklist:

Disaster recovery plan checklist item #1: Outline the goals of your disaster recovery plan

Any DR plan worth its salt outlines the goals or objectives of the plan — essentially, what you aim to accomplish. While the goals will vary depending on the needs of each organization, there are some universal goals that should be included. According to the IBM Knowledge Center, the following is a list of some of the major goals of a DR plan:

- "To minimize interruptions to the normal operations.
- "To limit the extent of disruption and damage.
- "To minimize the economic impact of the interruption.
- "To establish alternative means of operation in advance.
- "To train personnel with emergency procedures.
- "To provide for smooth and rapid restoration of service."



Other important objectives that should be mentioned include other business-specific priorities, adhering to industry compliance standards, and establishing **recovery time objectives (RTOs)** and **recovery point objectives (RPOs)**.

Disaster recovery plan checklist item #2:

Inventory all physical and digital assets

Having photographs of physical assets and up-to-date lists of all hardware, software, data, and security certificates is essential to disaster recovery. Be sure to identify critical applications and data, as well as the hardware required for them to operate. This also should include a list of any cybersecurity applications, certificates, extensions, and other cyber protection methods you have in place. The data can be broken down onto separate lists (tangible vs. intangible assets) for simplified organization. Here is an example of an inventory table for tracking some of your physical assets:

Company Disaster Recovery Inventory Profile

Type of Equipment	Manufacturer	Model	Serial #	Own/Lease	Cost
Laptop	Acer	Aspire R15	ABCD5DE555555555F55555	Own	$1,000
Server rack	Cisco	UCS C4200	ZYX55555WVUTS55555555	Own	$3,000

In disaster planning, the management of security certificates is often not considered a high priority — though, in reality, it absolutely should be. The cost of ineffective certificate and key management issues can have an average cost of $67.2 million for a single company over a two-year period, according to a study by KeyFactor and the Ponemon Institute. This statistic includes:

Average Cost of Certificate Management Mistakes

Event	Occurrences	Cost	Likelihood
Outages due to expired Certificates	4	$11,122,100	30%
Failed Audits/Non-Compliance	5.5	$14,411,500	42%
SSL/TLS certificate compromise	4.6	$13,423,250	39%
Code Signing certificate compromise	3.9	$15,025,150	29%
Rogue Certificates/MITM/Phishing	2.3	$13,219,850	38%

However, the potential costs to your company extend beyond finances. An expired SSL certificate alone can result in costs to your brand image, reputation, site downtime, and increase the likelihood of your business experiencing cyber attacks.

And as organizations grow and the number of connected devices increase, regularly applying and managing individual certificates becomes increasingly complicated and time-consuming. Whether you choose to manage these certificates with an in-house team or use a managed service provider, ensure that you maintain an up-to-date list of your certificates and renew them on time to prevent them from expiring.

Disaster recovery plan checklist item #3: Outline your data backup strategy and plan and perform data restoration tests

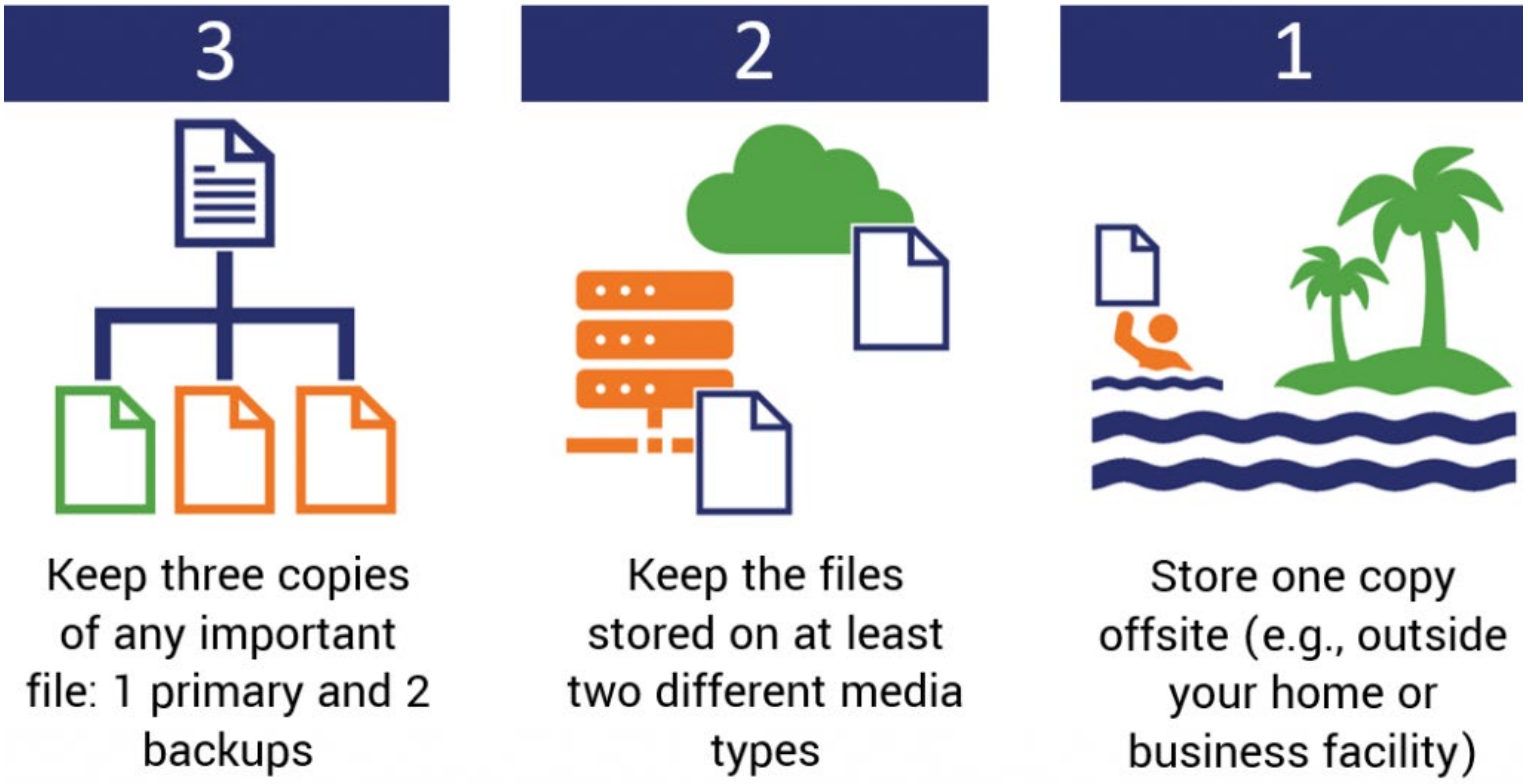
We cannot stress the importance of this component of our checklist enough: **Back up your data and test to ensure the restoration methods work**. Backing up all data aids in data restoration which helps your company get back up and running as quickly as possible. Accomplishing this gargantuan task does require a lot of forethought, strategy, and work in advance, but it will be well worth it when you find yourself in the aftermath of an event and you are able to bring your data and business back from the brink. And, with many automated systems

A successful disaster recovery plan includes a comprehensive data backup strategy that outlines:

- The types of information to back up,
- How frequently backups (and subsequent data restoration tests) should take place,
- Where the data backups will reside, and
- Who is responsible for implementing and storing the data.

Performing a data audit can certainly help this process. If you're an organization that already performed an audit to prepare for the European Union's implementation of the General Data Protection Regulation (GDPR) in 2018, then you're already ahead of the curve. However, it's vital to point out that audits should be performed regularly to ensure you have the most up-to-date information available. Also, be sure to **test your data backups regularly** to ensure they are in good condition and are reliable. Few things are worse than trying to use your data backups, only to discover that there is an error or another issue that prevents you from accessing your vital data.

A publication by Carnegie Mellon University and the US-CERT recommends following the **3-2-1 rule**:



- "3 — Keep 3 copies of any important file: 1 primary and 2 backups.
- "2 — Keep the files on 2 different media types to protect against different types of hazards.
- "1 — Store 1 copy offsite (e.g., outside your home or business facility)."

Ideally, you'll want to ensure that your data backups are saved in at least two separate geographic locations. This helps to make sure that your valuable and sensitive data won't be entirely wiped out in a disaster affecting the geographic area. For example, if your organization's office and local servers are physically located in California but you have data backed up to other servers located in Atlanta, Georgia, or Dallas, Texas, it means that you'll have a backup available should a natural disaster destroy the data at the California location.

Disaster recovery plan checklist item #4: List of all personnel and their DR responsibilities (if applicable)

Your organization's disaster recovery plan should include an up-to-date list of all employees. (This can be broken down by department for easy organization.) The general personnel list(s) should include the following information:

- First and last name
- Position/title
- Department
- Personal address
- Emergency phone number
- Email address
- Emergency contact information

Furthermore, your DR plan should go a step further and should include a list of who is responsible for what role in the event of a natural disaster or cyber incident. This disaster recovery team should include:

- Senior leadership,
- Service communications experts,
- IT security and IT services experts, and
- Public information/crisis communications personnel.

These individuals should be trained regularly to ensure that they understand their roles and are prepared to assume them after a disaster.

The personnel contact information list and disaster recovery team tree and list will be particularly beneficial for the next component of our disaster recovery plan checklist.

Disaster recovery plan checklist item #5: Develop a comprehensive communications plan

Creating a communications plan is two-fold: It should include both communications infrastructure technologies that enable your business to become operational as well as the actual communication of information to help keep employees, investors, and the general public informed.

For the first component, create a communications plan that includes alternative methods of communication and outlines how those systems will operate after disaster strikes. For example, you may want to implement preventative measures for your network by implementing network path diversity or using ad hoc networks. The benefit of the former is that if one network path is overwhelmed with traffic or if there is a point of failure in the physical conduit, using two or more types of network connections technologies helps to reduce the likelihood of both being disabled at the same time. The advantage of the latter is that ad hoc networks can be established relatively quickly and are particularly useful to emergency responders and organizations that are involved with public rescue and recovery operations.

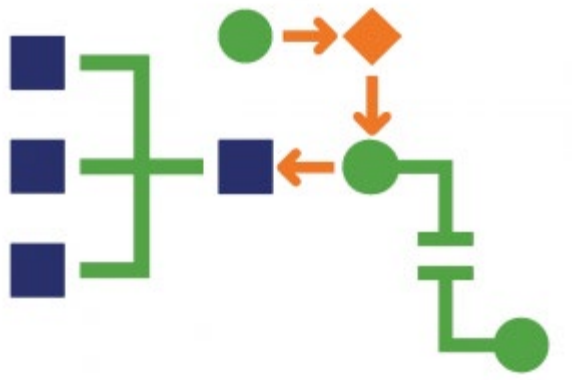
Having a crisis communications plan in place for your organization helps to keep everyone informed as well as increases trust and your brand image and reputation. Even just a quick communication that “there are no new updates or changes at this time” or that “we are currently working to resolve technical difficulties and get XYZ Company back to working for you” is better than operating on radio silence. The adage “no news is good news” does not necessarily apply during times of crisis — let people know that you’re there and are working to bring your business back to full operational

status. Create a few pre-approved statements with fill-in-the-blanks sections to tailor them to each specific emergency — these statements can be posted on your website, shared on social media, or disseminated to the media. Sharing these messages regularly in the aftermath of an event helps to reduce confusion and mitigate the spread of rumors and false information concerning your organization.

Lastly, a good communications plan — much like a disaster recovery plan or business continuity plan — should be reviewed and updated regularly to ensure that contact information, policies, and procedures are up to date.

Disaster recovery plan checklist item #6: Outline alternative work capabilities and redundancies

In the event of a natural disaster or even a non-environmental incident, getting your business back to operational status is a top priority. This may mean establishing alternative work capabilities for your employees as part of your disaster recovery plan — not necessarily just a backup physical location but also alternative options for your IT infrastructure, hardware, software, IT security, and communications capabilities as well. This way, employees can work remotely or from a secondary location almost as though there was no recent emergency.



One method for enabling secure communications is to use a virtual private network (VPN). VPN encryption helps to prevent third parties from “reading” your data by encrypting the information as it transmitted through the internet. There are two types of VPNs — those that use SSL/TLS protocols (SSL VPNs) and others that rely on internet protocol security (IPSec VPNs). The main difference between the two is that the latter VPNs use third-party hardware or software, whereas the former VPNs rely on the SSL/TLS protocols that already are equipped in most web browsers. According to Cisco, these “clientless VPNs” or “web VPNs” offer greater ease of use to end users because they only require a modern web browser.

Having a disaster recovery plan in place that specifies your corresponding alternative IT and communications capabilities and technologies will enable your employees to work securely while your traditional workplace is out of commission.

Disaster recovery plan checklist item #7: Outline how sensitive data should be handled

While ensuring that your communications and data are secure through the use of a VPN, it’s just as important to ensure that the sensitive information you wish to back up and use for restorations is also secure. A best practice for the secure backup and protection of your business’s and clients’ data is to use host-based or appliance-based data backup encryption methods. No matter which method of secure backup you choose, be sure to specify information about the method in your disaster recovery plan along with who is responsible for implementing it.

You should also implement in-transit encryption and at-rest encryption methods to protect your data. Much like how it sounds, in-transit encryption offers protection to data that is transmitting via the internet. SSL/TLS certificates are essential for protecting sensitive data while it is in transit through a secure, encrypted connection, such as when you are uploading data to a database or a storage server. At-rest encryption, on the other hand, is useful for protecting inactive stored data or data that is not in motion, such as when it is stored on a physical device, in a virtual database, or on a storage server. You can accomplish this by encrypting your sensitive files before uploading them to a device or virtual storage space. Both types of data encryption methods are essential to mitigate the risk of your data being stolen or compromised.

Disaster recovery plan checklist item #8: Ensure disaster recovery information is included in SLAs

Review the service level agreements (SLAs) you have with all third-party vendors — especially your backup data providers — and peer agencies (if you work for a local, state, or federal government organization) to ensure that they include information about how they will operate in an emergency. This should include information concerning:

- How quickly they will be able to get their operations back online;
- How quickly they will help you resolve your issues after a disaster;
- What percentage/amount of any monthly fees will be refunded/credited for affected services/downtime; and
- Credit/refund request stipulations, limitations, procedures, and timeframes.

If your company is the vendor for other organizations, the same can be said about what you should include in your SLAs with them. This way, they understand what your plan of action will be and how you will operate when your organization is recovering from a cyber attack or another disaster.

Disaster recovery plan checklist item #9: Keep your information up to date

Ensure your plan includes the most up-to-date information. Don't wait until an emergency strikes to realize that your personnel information, list of emergency contacts for the DR team, data backup information, or other

documentation are outdated. Make updating the disaster recovery plan and all corresponding information one of your standard organizational procedures to ensure that your IT and human resource teams perform these tasks on a regular basis.

Disaster recovery plan checklist item #10: Test your plan and procedures regularly and conduct exercises

While this may seem like a no-brainer, it's both amazing and concerning just how few organizations fail to abide by this basic rule. According to a press release on the Ponemon Institute and IBM's study on organizational resilience, most organizations create plans but fail to test them:

> *"Of the organizations surveyed that do have a plan in place, more than half (54%) do not test their plans regularly, which can leave them less prepared to effectively manage the complex processes and coordination that must take place in the wake of an attack."*

This concept is much like buying roll-down hurricane shutters to protect your business's windows but never bothering to install them or test to ensure they work: These devices may look nice in their new condition, but they won't do you any good during a storm if they just sit in a storage unit and aren't used to protect your building. Regularly test your plan to ensure that your contact lists, procedures, and everything remains up to date so you and the disaster recovery team are ready when a disaster strikes.

Final thoughts and resources for disaster recovery planning for IT professionals

We hope that you've found the information in this disaster recovery plan checklist informative and helpful. As you've seen throughout this post, your disaster recovery plan is a living document that needs to be continuously revisited to ensure it is up to date, compliant with NIST or ISO standards, and ready to serve as your proverbial lighthouse in the storm.

In addition to our disaster recovery plan checklist, here is a list of some additional resources that may be of use when creating an IT disaster recovery plan:

- NIST's Computer Security Resource Center — particularly:
  - Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-84 Rev. 1)
  - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (NIST Special Publication 800-84)
- Microsoft Premier Field Engineering Disaster Recovery Planning Template — This Word document serves as a great resource that can be customized to meet your organization's needs.
- The government of Alberta, Canada's Ministry of Education website — This IT Disaster Recovery Planning Guide provides a valuable basic template that can be adapted to fit the needs of other organizations.
- The National Mining Association's (NMA) Media and Community Crisis Communication Planning Template

— This is a great example of a crisis communications plan template that can be used to help you create a plan.

- DisasterRecoveryPlanTemplate.org website — This site serves as a valuable resource for a variety of plan templates, including IT disaster recovery plans and business continuity plans.

As always, we invite you to share your thoughts and insights on this topic in the comments below.

#CYBER RECOVERY #CYBER RESILIENCE

Be the first to comment

Leave a Reply

Your email address will not be published. We will only use your email address to respond to your comment and/or notify you of responses. Required fields are marked *

Comment

Name *

Email *

Website

☑ Notify me when someone replies to my comments

Captcha *

3 − = 0

Post Comment

Author

Casey Crane

Casey Crane is a regular contributor to Hashed Out with 10+ years of experience in journalism and writing, including crime analysis and IT security. She also serves as a Content Marketer at The SSL Store.

Recent Posts

A Sneaky Online Security Threat: Encrypted Malware in SSL

October 24, 2019

New York SHIELD Act: The Latest Amendment to NY State's Cybersecurity Law

October 23, 2019

Post-Quantum Cryptography: 10 Things You Need to Know

October 17, 2019

What Is a DDoS Attack? (Hint: It Involves Zombies & Traffic Jams)

October 14, 2019

Browser Updates Round-Up: Continuing the Push for HTTPS Everywhere

October 8, 2019

Follow Us

Free Ebooks

Email Security Best Practices – 2019 Edition

Download Now

Certificate Management Best Practices Checklist

Download Now