Ransomware 101:
What to Do When Your Data is Held Hostage
Forward

Information is the lifeblood of our economy. It enables us to run our businesses more efficiently, to sell smarter, to create new products we never could have imagined even a decade ago. Our digital economy has also revolutionized the business of cyber crime. Instead of stealing information and going to all the trouble of selling it or using it themselves, cyber thieves are simply holding our systems and our precious data hostage and demanding ransom for their release. For thieves, it’s the perfect crime: ransomware is much harder to spot and prevent than other malware, and they get near-instant payoff in untraceable cyber currency. For the victims, it’s the perfect storm. As opposed to a typical data breach, where business operations can continue while you sort things out, everything grinds to a halt, and even after ransom is paid, there can be days or weeks of system cleanup. It’s no wonder that, from attacks against medical centers in the headlines to television techno-dramas, ransomware is big, bad news.

On the positive side, there are ways to protect your organization against the 100,000 new variants of ransomware that are released every day. Forewarned really is forearmed, so in this eBook, we take you on a tour of the ransomware world: the software, the criminals, and their tactics; the thorny question of whether or not to pay ransoms; ways to prevent or mitigate the threat; and a real life account of a ransomware attack and how it was stopped. Just in case, we even give you the ins and outs of paying in cyber currency.

Read on and be ready.

Contents
Forward .................................................. 2
How Ransomware Could Hold Your Business Hostage ................. 3
Trading in Fear:
The Anatomy of Ransomware ............................. 6
“Don’t Panic!”: Lessons to Be Learned from Ransomware ............ 9
 Tradable, Untraceable, Sometimes Unavoidable: The Business of Bitcoin ........ 12
About the Author ........................................ 14
Helpful Links & Resources .............................. 15

About This Document
This document is intended to provide you with general information about ransomware, a type of malicious software that threatens to publish the victim’s data or perpetually block access to it unless a ransom is paid. This information is not intended to be or replace legal advice. Please seek out your legal counsel for such advice.
How Ransomware Could Hold Your Business Hostage.

By Doug Pollack, Chief Marketing Officer, ID Experts

Put yourself in this picture: Your organization has a pretty good handle on data security. You have a secure firewall and good anti-malware software running on your systems. You monitor network traffic for suspicious activity. You’ve trained your staff in good cyber hygiene, and reviewed your business partner contracts to make sure they’re doing their part to protect sensitive data.

It’s “patch Tuesday,” your automated scripts are installing the latest security updates to your software, and you’re feeling pretty good until a staff member calls and reports problems accessing a data file. The next thing you know, ransom messages start popping up on user screens all over the company demanding payment to access their own data. Suddenly, you can’t control the digital information that is the lifeblood of your business, operations grind to a halt, and you have to make some hard decisions.

If you haven’t experienced ransomware yet, it’s probably just a matter of time. For cyber criminals, it’s an almost-perfect crime. For organizations and individuals, it’s their worst nightmare, and it’s just getting started. In this new series of articles, we’ll look at the epidemic of ransomware: what is it, how does it get into your systems, and what you can do about it.

Holding Data Hostage

Since the medieval highwaymen and the heyday of Al Capone, criminals have used extortion to hold hostage the safety and property of others. Ransomware, the latest generation in that long criminal tradition, gains access to a computer system and makes either the system or the data inaccessible, then attempts to extort payment from the owner in return for returning access. Often there is a limited time to pay, after which the data will be permanently lost, and the payment is typically in some kind of untraceable cyber currency such as Bitcoin.

Ransomware began to make national news in February 2016, when the Hollywood Presbyterian Medical Center had to pay $17,000\(^1\) in Bitcoin to ransom its system,
followed by a string of attacks on other healthcare providers. But the problem is already widespread enough that a number of security experts have already declared 2016 the year of ransomware and digital extortion. Organizations of all types and sizes, from consumers to small businesses, law firms, and even police departments have fallen victim.

Like other protection rackets, ransomware is a high-profit strategy for criminals. There are multiple steps to monetizing personal data, intellectual property, or other sensitive information that is stolen outright. It is often “fenced” on the Dark Web, then the buyer has to turn it into a false identity that can be used to fraudulently obtain goods or services. With ransomware, on the other hand, the victim has to pay the criminal directly, the payment happens within hours or days in untraceable currency, and there is no chain of custody to point to the criminals because the data stays on the victim’s system the whole time. And PC Magazine recently quoted OpenDNS Security Analyst Kevin Bottomley’s finding that ransomware usually takes less than three minutes from infection to encryption time.” As Brian Contos, VP and Chief Security Strategist at Securonix, has said, “[Ransomware] is a volume business. It’s simple, relatively anonymous, and fast.”

Ransomware is Big Business

With quick payoff and no risks to the criminals, ransomware is spreading like the plague that it is. A McAfee report found that new ransomware samples grew by almost 50 percent between the first and second halves of 2014, then jumped by over 5 times, to more than 2 million samples, in the first half of 2015. At that rate, hackers are releasing over 100,000 new ransomware variants daily. No wonder security software vendors can’t keep up.

The FBI estimated that losses for victims from a single strain of the Cryptowall malware were close to $18 million. Multiply that by the millions of variants that are now being released each year, even allowing for less successful ones, and it’s clear that ransomware is taking a huge bite out of the economy. And ransom estimates alone don’t take into account the costs of business that may be lost during the hours or days that systems are locked, the costs of repairing or restoring systems—even if the ransom is paid, administrators will want to ensure that the ransomware is removed—or the dire costs, including possible loss of life, when critical systems such as healthcare or energy control networks are held hostage. TechNewsWorld reported recently that 72 percent of companies infected with ransomware could not access their data for at least two days because of the incident, and 32 percent couldn’t access their data for five days or more, and the costs of downtime often exceed the cost of ransom.

Is Hostage Data Breached?

A cruel irony of ransomware is that it could also be considered a data breach, even though the data never leaves the victim’s systems. At the recent 2016 Healthcare Compliance Association conference, Iliana Peters from the Department of Health and Human Services’ Office for Civil Rights (OCR) pointed out that HIPAA regulations define a data breach as “impermissible acquisition, access, use or disclosure of PHI (paper or electronic) which compromises the security or privacy of the PHI.”

“[Ransomware] is a volume business. It’s simple, relatively anonymous, and fast.”

— Brian Contos, VP and Security Strategist at Securonix
She then went on to note that data doesn’t need to be exfiltrated in order for an incident to be a notifiable data breach. In a ransomware attack, healthcare providers and others that handle protected health information will need to conduct the required four-factor incident risk assessment to decide whether breach response and notification are required. I suspect that OCR will be providing greater guidance in this somewhat gray area in the future.

Since ransomware on a mass scale is a new phenomenon, there is no precedent to tell us whether any given ransomware attack may ultimately be considered a data breach. But healthcare is not the only industry covered by a complex network of federal and state regulations regarding privacy and data breaches, so businesses shouldn’t rule out the possibility. Even as decision-makers and security staff are scrambling to deal with the immediate threat of a ransomware attack, privacy and compliance staff will have to consider carefully whether to treat the incident as a breach, with all the effort and additional costs that would entail.

Fighting the Ransomware Mob

The gangster Al Capone once said, “A crook is a crook, and there’s something healthy about his frankness in the matter.” Ransomware attackers are evolving their tools and their business models fast, from ever more efficient malware to ransomware for hire and “customer service” capabilities that help victims unfamiliar with cyber currencies to make payments. They’re smart and agile, but in the end they are just crooks, and a concerted effort by security experts, law enforcement, and informed, prepared organizations will eventually stem the tide of ransomware. In the meantime, knowledge is your best defense, so in the rest of this series, we’ll look at different types of ransomware, where it comes from, how it works, and how you can fight it.
Ransomware is an epidemic. Every day more businesses, consumers, government and other organizations are finding their critical data held hostage and collectively paying millions of dollars to get it back. In some cases, such as attacks on hospitals, it’s literally threatening lives. And with over 100,000 new variants released every day, ransomware is mutating like a nightmare virus, while the world’s cyber security forces work feverishly to stop it.

As with Ebola and Zika and other viral epidemics, experts and potential victims need to understand how the disease attacks and how it spreads so they can protect themselves. In our first article in this series, we looked at the basics of ransomware and its costs to business and consumers. In this article, we’ll look at some of the “strains” of ransomware and how it infects computers, networks, and other devices, to help your organization practice safer cyber hygiene.

Ransomware in a Nutshell

Most ransomware either locks the interface or encrypts files on a computer or network, sends users a ransom message, and, ideally, releases the interface or decrypts the data after the ransom is paid. (Although Richard Walters, senior vice president of security products at Intermedia, recently told TechNewsWorld that companies have a 20% chance of not getting their data back after the ransom is paid.) The details of ransomware can and do vary widely, partly to keep attackers ahead of security experts and partly to keep victims off balance and paying.

According to The ICIT Ransomware Report, the first ransomware appeared in the 1980s, and, ironically, until ten years ago, most of it was fake. Fraudulent spyware removal tools and performance optimizers scared users into paying to fix problems that didn’t really exist. Although the first ransomware that actually denies access to data was developed in 1989, the malware didn’t become common until 2006.

At this point, there are two major types of ransomware:
• **Locker ransomware** restricts user access to infected systems by locking up the interface or computing resources within the system. It puts up a display page telling victims to pay through credit vouchers purchased from local stores or money transfer services. According to security software vendor Symantec, locker ransomware accounted for about 36 percent of ransomware samples they detected in 2014-2015. Attackers have moved away from locker ransomware because the disabled interface prevents victims from paying in crypto currencies such as Bitcoin, which are faster and less traceable, so better for the recipients. However, experts expect that locker ransomware may regain popularity with attackers because it can affect mobile devices and devices on the “Internet of things.”

• **Crypto ransomware** encrypts files on the target system so that the computer is still usable, but users can’t access their data. It typically uses strong industry-standard encryption schemes, often with encryption keys that time out, adding urgency to the ransom payment deadline. Crypto ransomware leaves the user interface functioning, so that users can get to the Internet to make ransom payments in crypto currency. Symantec say that crypto ransomware makes up 64 percent of the samples that their software detects.

The success of any given ransomware variant depends in part on the technology and part on how skillfully the attackers are able to exploit the fears of the victims. On the technical side, successful ransomware needs to evade detection by security software long enough to install itself and do its dirty work, and it needs to employ locking or encryption strong enough that it can’t be easily broken. But powerful ransomware is now widely available on the Dark Web for free, so any “script kiddie” (a technically unsophisticated would-be hacker) can mount an attack in return for giving the developer a share of the profits. The successful cyber-extortionist is also able to work the psychological scam, scaring victims into paying rather than taking defensive measures, and giving them reasonable confidence that their systems will be restored plus enough technical support that they can figure out how to pay in cyber coin.

**Ransomware Attack Vectors**

As with other malware, the spread of ransomware often depends on user ignorance, but cyber-extortionists have come up with a few new tricks to infiltrate systems. Ransomware enters systems through four main channels:

• **Social engineering:** Ransomware is often downloaded by unwitting users. Phishing emails induce users to click on bad links or download and open malicious attachments. According to the ICIT report, criminals will hire services to redirect users from adult content sites or media piracy sites to their downloads (adding shame to the urgency of fear when the user is trapped) or they will use malvertisement services to bait users from ads on legitimate web sites. Bad guys are also now using social media messaging as an attack vector for malware. This is harder for organizations to defeat because the attacks are now running under HTTPS/SSL, so that it’s harder to detect the malware.

• **Layered attacks:** Criminals who have already infected a system sometimes sell access to ransomware

“Powerful ransomware is now widely available on the Dark Web for free.”
criminals. The undetected malware on the so-called “zombie” machine can download the ransomware and remain after the ransom is paid, waiting for another opportunity to steal data or extort payment.

- **Embedded**: Ransomware is sometimes embedded in seemingly legitimate downloads such as software updates or resume files. Fake Adobe Flash updates are a notorious Trojan horse for delivering ransomware because Flash is so ubiquitous in browsers around the world. As this Symantec post shows, the fake update pages can be very convincing.

- **Self-propagation**: Once inside a network, some ransomware can seed itself to additional computers or other devices via SMS messages or a user’s contact list.

While user awareness can help deter the spread of ransomware, the other three sources are more difficult to isolate and stop.

**Fighting Fear Itself**

At this point, the technology behind ransomware is formidable, as developers employ stronger encryption and more tactics to elude detection. Eventually, security technology will catch up, but in the meantime, organizations and individuals need to avoid giving in to fear because that is the ransomware criminal’s greatest weapon. Just as the earliest forms or ransomware extorted users with non-existent threats, much of today’s ransomware is not as invincible as it seems, which is why attackers keep coming up with scarier tactics for their malware. One of the most brutal is the Petya virus, described in a recent Kaspersky blog. Not only does the malware attempt to lock the whole hard drive at once rather than slowly encrypting individual files, its user interface is a grinning skull and crossbones made mostly of dollar symbols.

While there is no perfect defense against ransomware, there are remedies that your organization can try before facing the ultimate question, “To pay or not to pay.” In the final article of this series, we’ll look at preventions, some possible ransomware cures, and steps you should take after the crisis has passed.

---

If you’ve ever watched a detective show, you know a murderer suspect must have a motive, a means, and an opportunity to commit the crime. If we think about ransomware—malware that holds computers or data hostage—every cyber criminal on the planet has all three.

As we discussed in our first article in this series, hackers can make millions of dollars off a single strain of ransomware, so the financial motive is strong. In our second, we learned that the means for a ransomware attack are available to even the most unsophisticated criminals in return for a small cut of the action, and opportunities to deliver the malware abound, from phishing attacks against users to embedding it in legitimate software patches. It’s no wonder that businesses and consumers are falling victim, and the worst part is that, as fast as systems can be resurrected, they can be “murdered” again. (I know, this is starting to sound less like a detective story than a season finale from Game of Thrones.)

Until the security community figures out how to stop it, ransomware infections may be as inevitable as death and taxes. But the better you handle them when they happen, the less chance you will be plagued by them over and over again. In this article, we’ll look at things you can do to lower the likelihood of a malware attack, and how to handle one if it happens, both during the attack and after.

Building Your Defenses

Obviously there is no perfect defense against ransomware. If there were, attacks wouldn’t have increased by orders of magnitude in the last couple of years. That said, there are steps you can take to reduce the risk. Training staff to spot and avoid phishing scams and not to open unsolicited email attachments will help keep ransomware out, and, according to a study by Ponemon Institute, it can have up to a 50x ROI by preventing multiple types of attacks. Keeping software up to date helps stop attacks that take advantage of known vulnerabilities. Infosec experts also recommend a layered approach to security that includes firewalls, web scans, and anti-virus software.
Prevention is great, and it will fend off some percentage of ransomware attacks, but your most important defense against ransomware is mitigation—planning ahead to limit the damage and to help recover quickly from an attack. You can limit the damage by segmenting systems and networks and by a rigorous system of access controls that ensures that users only have access to information and services that they need, limiting the potential damage from a stolen password. And the key to recovery is to have backups that are complete, up-to-date, disconnected from your systems (either physically or in the cloud), and tested regularly to be sure that you can successfully restore from them.

Calm Under Fire
With the current explosion of ransomware, there’s a good chance that a ransomware attack will get through, despite your best defenses. Unfortunately, there are so many strains of ransomware and so many different attack tactics that no one can tell you exactly what to do when faced with the CryptoWall doomsday clock or the Petya pirate flag. But here’s what not to do: panic.

One of our associates, an IT consultant, dealt with a ransomware attack recently at a client of hers. Her story demonstrates many of the things that you should do, starting with keeping calm. This consultant (at her request, I’ll just call her “D.”) provides IT services for smaller companies that don’t have their own IT staff. Recently she was contacted by an employee at one of her clients, a manufacturing company with around 50 employees, who said the files on her computer were suddenly changing names. She sent a screen grab showing the altered filenames, so D. did a quick Google search and discovered that a ransomware attack was in progress.

The ransomware was still in the process of encrypting files and hadn’t displayed a ransom screen yet, so D. told her client to immediately disconnect the affected server from the network, disconnect all servers from the Internet, and tell all employees to stay off the network and not open any files until she could assess the situation. When she arrived on site, she found the main server was totally corrupted and was seeking files shares on the network to encrypt more data. At that point, the client’s business was badly disrupted, so a decision was made not to do forensics to track the source of the attack, and instead to try to restore the systems from backups. Even without forensics, it took 48 hours to fully recover from the attack.

D. has a lot of takeaways from the ransomware attack and its aftermath. First of all, she and her client did a lot of things right. “All the servers were backed up both to NAS servers and to the cloud, so we could restore the systems and get everything back on track with no business loss to my client. We also didn’t panic and pay a ransom. I suspect that paying gets you listed on the Dark Web as an easy target, setting you up for more attacks. Instead, we spent the money on next-generation security software that made it much easier to detect and cleanup the malware in my client’s system and will help me spot and stop attacks in future. Thank goodness we spend money on that instead of paying ransom.” Things she learned? “We could have restored the systems faster if I had told everyone to stay off the systems entirely and go to paper-based work until things were back to normal. It’s an inconvenience, but it would have speeded up the recovery. We also

Victims of Petya ransomware are all too familiar with this skull and crossbones graphic. Pressing any key takes the user to instructions for paying the ransom.
discovered some files on the network that had been created outside the file server and hadn’t been backed up. We had to get those off the network first, for safety, what had to be kept. So in future, we’ll be encouraging users to keep everything where it will be backed up. And I’m also considering a backup strategy for the NAS servers.”

If your organization is faced with a ransomware attack, do what D. and her client did:

- **Don’t panic!**

- **Don’t turn off systems** (that can make things worse), but do isolate them from the network and the Internet.

- **Do get online and do your research.** At least you can find out what kind of malware you’re dealing with, and you may find decryption and other tools available to help restore your systems.

- **Don’t let scare tactics push you into paying** the ransom before you’ve explored other options.

The ransom decision can be a tough one. Like D., the FBI warns⁴ that paying ransom encourages this kind of criminal activity. On the other hand, if you’re in a situation like the recent attack on Hollywood Presbyterian Medical Center⁵, and lives may be at stake, you have to balance those risks. In any case, take the time to find out what you’re dealing with and to assess the your options and risks before making the ransom decision. If you have good backups and can recover quickly, you may not need to pay at all.

Be an Unequal Opportunity Target

The only possible upside to the ransomware crime wave is that it may be the tipping point that drives businesses to prepare for the worst, be it malware attack or data breach. (In the Ponemon Institute’s Sixth Annual Benchmark Study Privacy and Security of Healthcare Data⁶, ransomware attacks ranked #2 out of all cyber attack concerns.) D. says her client has a new resolve and commitment to creating a really solid incident response plan, because this incident made it clear that attacks aren’t 100 percent preventable. “These systems had good firewalls, anti-virus, and anti-malware software running, but it obviously wasn’t enough. And while we didn’t get to do forensics, the files began to be encrypted just after the weekly software updates started, so the ransomware was probably introduced through a software update, not a user error.”

There are so many yet-to-be-answered questions about ransomware: What tactics will hackers try next? How can we stop it? Is it a breach? When to pay and when not to pay? The only certainty is that criminals will continue to have motive and means to attack for the foreseeable future. The best we can do is to limit their opportunities through user awareness, choosing the best cyber-security we can afford, and through preparation that enables us to respond and recover as efficiently as we can. The more we can keep ransomware from being a fast track to riches, the less criminals will invest in its future.

---

2 https://info.wombatsecurity.com/cost-of-phishing
3 http://www.precisesecurity.com/wp-content/uploads/2014/05/cryptowall.png
4 https://blog.kaspersky.com/petya-ransomware/11715/
5 http://www.databreachtoday.com/blogs/please-dont-pay-ransoms-fbi-urges-p-2120
6 http://money.cnn.com/2016/02/17/technology/hospital-bitcoin-ransom/
In recent articles, we’ve talked about the epidemic of ransomware, how it works, and the thorny question of whether to pay. What often catches organizations by surprise is not only the ease with which ransomware can bring operations to a halt, but the difficulty of paying the ransom if you determine that that is your best option.

The currency of choice for cyber extortionists is Bitcoin, a digital, completely virtual form of money that can fluctuate wildly in value, offers no protections, and can open you up for other kinds of cyber theft. Most businesses are completely unfamiliar with this "cryptocurrency," but if you’re considering paying a ransom, the dangers of Bitcoin should figure into your choice. So let’s look at some Bitcoin basics. (First basic: “Bitcoin” is used to refer to the whole system of currency, whereas “bitcoins” are individual units.)

Why Bitcoin is Not Your PayPal
Many of us are familiar with PayPal, which allows people to transfer regular money conveniently on the web. A PayPal account can be pre-loaded with money to make a payment, or it can be tied to a credit card or bank account. The payment is either deducted from your PayPal balance or it will show up on your bank or credit card statement at the end of the month.

While PayPal transfers money, BitCoin IS money—virtual money that exists as a series of transaction records kept by individuals or organizations in a Bitcoin “wallet” (an application) and recognized by other Bitcoin wallets. The value of a bitcoin also fluctuates versus other currencies. So if your organization is hit by ransomware and you have to pay in bitcoins, you have to go to a Bitcoin exchange such as Coinbase, pay dollars for bitcoins at the going rate, and then deliver those bitcoins to the extortionists. Which all sounds straightforward until you dig into the details.
What Could Go Wrong?

Unlike most other forms of payment, Bitcoin is completely unregulated. There is no central issuer of bitcoins, and there’s no Federal Reserve of bitcoins that keeps track of all the transactions or controls their value. Bitcoin transactions are untraceable. That’s why it’s the preferred currency of the Dark Web, and why there are so many risks in using it.

The first risk is in buying bitcoins. While there are a few Bitcoin ATMs where you can buy the coins in cash, if there isn’t one near you, or if your organization isn’t prepared to come up with thousands of dollars in cash on short notice, you will need to buy bitcoins from an online exchange. The exchange will require you to supply a bank account or debit card number to fund the transaction, which creates an immediate risk because Bitcoin exchanges are notorious for being hacked. (One of the earliest, Mt. Gox, went bankrupt after it was hacked in 2014, losing an estimated $450 million worth of its customers’ bitcoins.) The last thing you want is hackers getting away with your organization’s bank account numbers, so if you have to buy bitcoins for a ransom, set up a new bank account to hold the payment funds and close the account as soon as possible afterwards.

The second risk is that bitcoins fluctuate in value, whereas ransomware demands are usually specified in fixed dollar amounts. You can check the value of the coins when you buy, but there is no guarantee that if you buy, say, $10,000 worth of Bitcoin, it will be worth that amount by the time you turn it over to the attackers. And if you don’t meet the extortionists demands with the full amount by the deadline, they may not release your systems or data. Cyber extortionists want to be able to pay ransom successfully (because if it doesn’t work, people will stop paying) and some provide customer service which victims can contact to negotiate, but it may be wise to just buy some extra Bitcoin, just in case you have to come up with extra at the last minute. Theoretically, you can cash it in later for whatever it’s worth at that time (assuming the exchange doesn’t get hacked).

The third risk is that you have no leverage with the attackers once a ransom is paid. When you pay with credit cards or PayPal, you can challenge a payment and get it credited back by the seller. With Bitcoin, once the money is paid, it’s gone, the attacker is gone, and if they don’t release your computers or data, or if they left hidden malware so they can turn around and ransom them again, you’re out of luck. Again, smart attackers won’t skip out without your funds because if word gets around, people will quit paying. But since any petty hacker can now get in the ransomware game, you can’t assume that they’re all smart. You have to decide whether losing those funds for nothing is an acceptable risk.

Now How Much Would You Pay?

If a ransomware attack brings your operations to a halt, you have to weigh the costs of paying versus trying to resurrect your systems and data yourself. Realistically, you want to restore everything from clean backups anyway, to minimize the possibility that there is still hidden malware stealing data in the background or waiting to take your systems down again. But if you’re providing time-critical services such as healthcare or controlling a nuclear power plant, you may choose to pay a ransom so that you can continue operations now and restore systems as business demands allow.

Either way, the risks and vagaries of bitcoin payments should figure into your decision. And if you do decide to pay, pay carefully.
About the Author

Doug Pollack
Chief Marketing Officer, ID Experts

As chief marketing officer, Doug is responsible for the strategic direction and marketing of our innovative software and services. He has over 25 years of experience in the technology industry, having held senior management and marketing roles with Apple, Inc., 3Com Corporation as well as several venture-backed enterprise software startups. He holds a BS in Electrical Engineering from Cornell University and an MBA from the Stanford Graduate School of Business.
Helpful Links & Resources

The Growing Threat of Ransomware, PG Mag

2016 Threats and Predictions, McAfee Labs

The ICIT Ransomware Report, ICIT

The Cost of Phishing & Value of Employee Training, Wombat Security
https://info.wombatsecurity.com/cost-of-phishing

Please Don’t Pay Ransoms, FBI Urges, ISMG: Data Breach Today

Bitcoin Converter, CoinDesk
https://ocportal.hhs.gov/ocr/breach/breach_report.jsf

List of State Security Breach Notification Laws
http://www.coindesk.com/price/

The Cyber-Crime Super Highway - A Tour of the Dark Web
https://www2.idexpertscorp.com/blog/single/the-cyber-crime-superhighway-a-tour-of-the-dark-web

Ransomware in Healthcare - Where the Stakes are Higher
https://www2.idexpertscorp.com/blog/single/ransomware-in-healthcare-where-the-stakes-are-higher

Fight Fire With Fire - Grasp the Economics of Cyber Crime

Study: Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2016

Breach Response Buyer’s Guide

ID Experts Knowledge Center
https://www2.idexpertscorp.com/knowledge-center

Products & Services
Breach Response Services
https://www2.idexpertscorp.com/products-services/breach-response-service/

Identity Protection Services
https://www2.idexpertscorp.com/products-services/identity-protection-services/

Pre-Breach Services
https://www2.idexpertscorp.com/products-services/pre-breach/