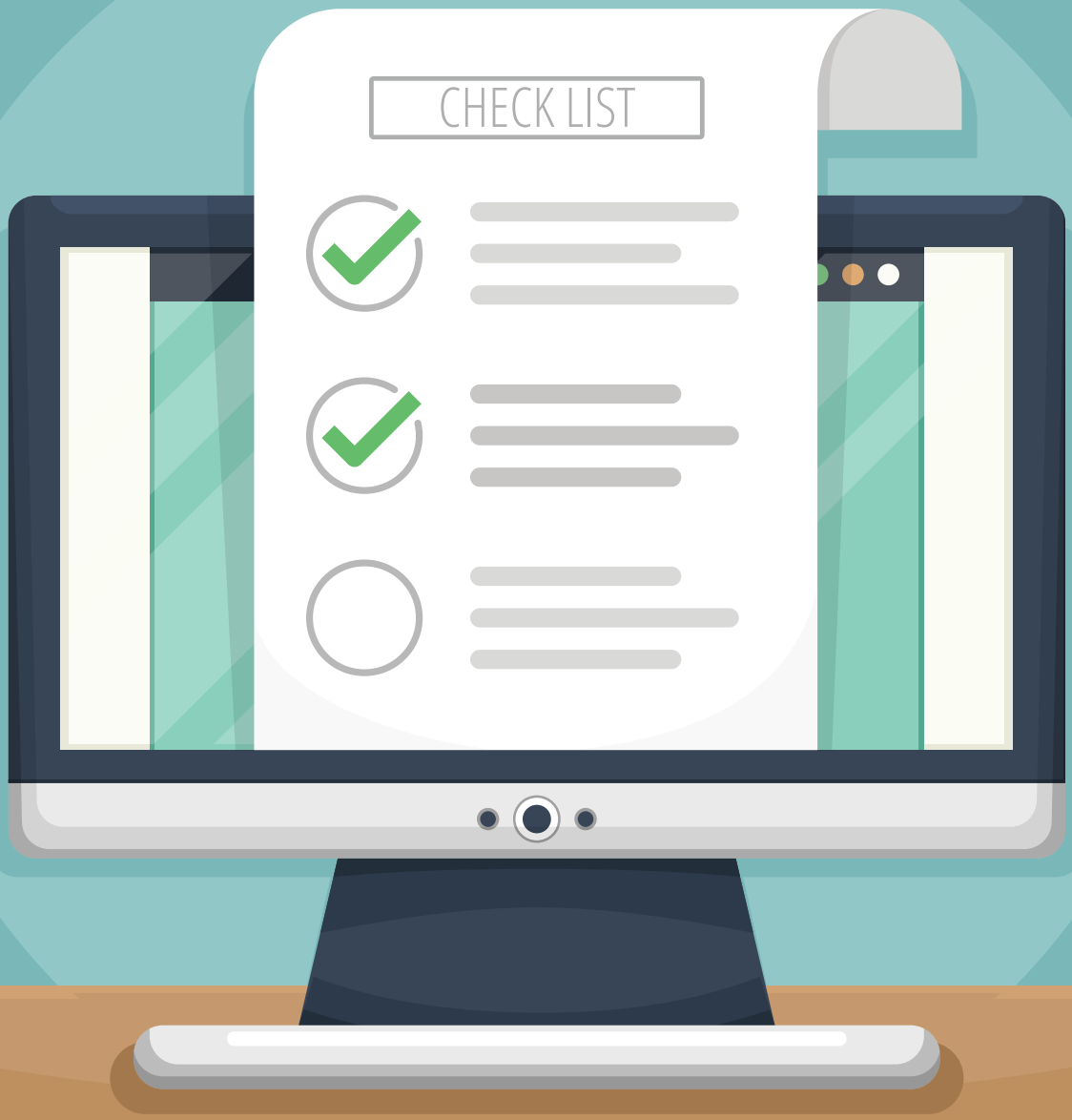
CYBERSECURITY CHECKLIST FOR LAW FIRMS



CYBERLINK**ASP**

In today's world, security breaches are on the forefront of companies minds more than ever before. From large organized hackers to the rouge employee, there are a wide variety of threats threatening the integrity of a firm's data today.

With invaluable data on every hard drive, a cyber security breach could wreak havoc on your systems and destroy your firm's reputation. As a law firm, it is your responsibility to ensure your client's information remains secure.

WHO WANTS YOUR INFORMATION

While it may be hard to visualize possible cyber intruders, they are closer than you may think. In order to understand how to best protect your data, you must understand who is trying to get a hold of your information and the techniques they are utilizing to do so.

So, who's after our information?

The answer: lots of different people; and none of them are ones we'd want to have it.

WHO WANTS YOUR INFORMATION

Organized Crime Syndicates

These are organized groups of criminals who band together in an effort to retrieve confidential information digitally. For instance, one of the most famous and feared groups of hackers today is Anonymous. They have hacked governments, agencies, and even the Church of Scientology.

Terrorist Organizations

Militant groups such as the Islamic State are not only known for their physical terrors; they also attack digitally. Hundreds of small business and firms have suffered from unforeseen attacks from militant groups.

Foreign Nations

When glancing at the news today, it's not hard to see that many governments have been accused of sponsoring cyberattacks. In the Sony hacking of 2014, North Korean hackers carried out a damaging strike on the media giant.

WHO WANTS YOUR INFORMATION

Insiders

Unfortunately, not all attacks come from the outside. Thousands of companies have suffered from employees compromising their information. In 2015 alone it cost companies a total of $1.2 billion dollars.

Hacktivists

A hacktivist is a someone who hacks to serve some personal or political cause For instance, one of the most famous and feared groups of hacktivists today is Wikileaks. They were able to release thousands of emails in the 2016 election to damage a candidates reputation.

Common Criminals

Many criminals no longer lurk in dark alleyways - they might prefer a desktop in their basement these days. And it’s much easier to hide on the vast internet than it is to hide on city streets.

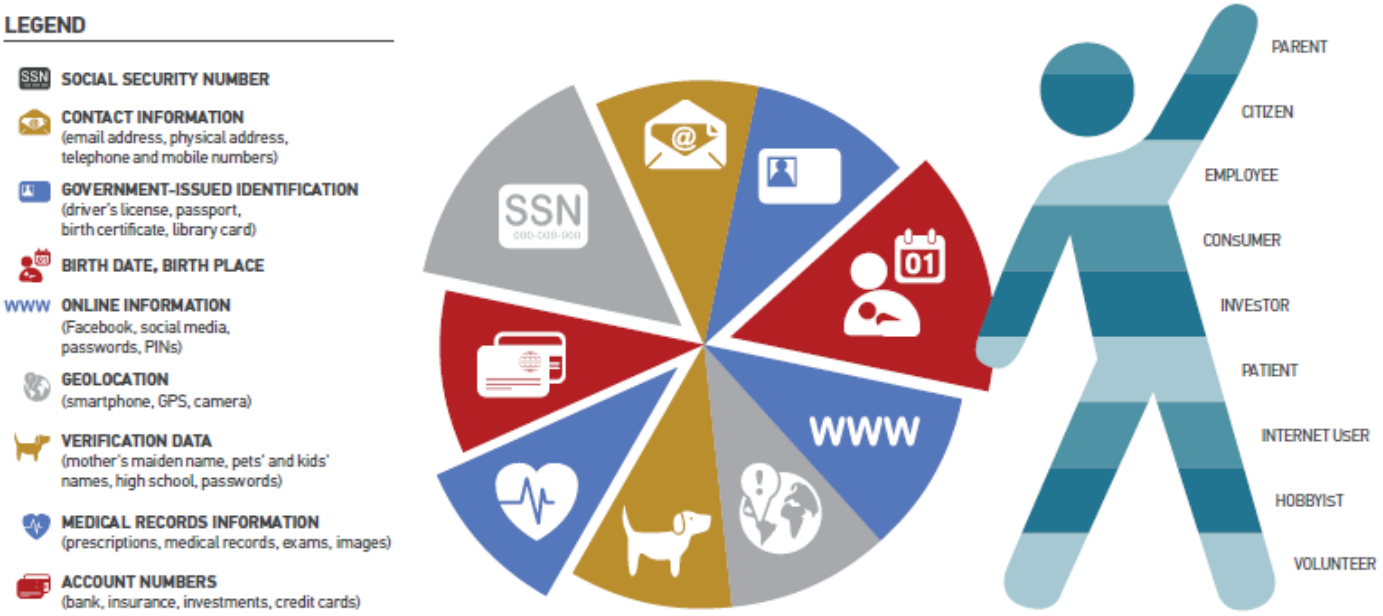
So what are these criminals looking for anyways?

They want to find Personally Identifiable information (PII for short). PII is any information that can lead to locating, contacting, and uniquely identifying an individual. Keep in mind that PII includes both data that by itself distinguishes an individual and multiple pieces of data that can be combined to identify a unique individual.

For instance some fairly common pieces of PII are your full name, Social Security Number, Address and phone number, Vehicle Registration Number, and Biometric information (like height and weight). Anything hackers can use as a way to identify you as an individual would be considered PII.

YOUR **PII CHART™**

Take time to inventory the identity relationships you have with the companies, organizations, and individuals you entrust with your personally identifiable information or PII. See how your identity is a PII Chart™, a picture of relationships you've created. Once you visualize the slices of your PII, managing your identity assets becomes easier.



COMMON WAYS YOUR INFORMATION IS COMPROMISED

Hackers have become more creative as the internet has become more sophisticated and people have become wiser about how they store their data. They have developed many techniques in order to collect data from unsuspecting victims.

One of the most common tactics they utilize to retrieve your data is social engineering. These are not stereotypical things you think of when hacking comes to mind. These types of hacks trick people into surrendering confidential information. While many believe they are not easily fooled, these hackers use an array of strategies to fool people and tend to be fairly successful.

It's even more favored when the targets are institutions with lots of employees: Verizon's analysis of security breach in 2012 found that while only 7% of all breaches were caused by social engineering, it was responsible for 22% of those affecting larger companies. People are by far the weakest link in any firms security program.

Rather than exploiting flaws in a system, social engineering exploits the flaws of the people with access to that system.

The larger the system, the more weak links, flaws, and vulnerabilities there are to take advantage of. Social engineering preys on good intentions. You might know not to share PII with unauthorized users, but what if you think a request for information is coming from a trusted person? Once cybercriminals have used social engineering to obtain PII, they can impersonate authorized users and bypass access controls to a system. Identity theft, leaking of customer data, and loss of system controls quickly ensues.

Four Main Species of Social Engineering:

Phishing is a catchall term referring to unsolicited email requests to provide information, click on an infected link, or visit a compromised website. It's not unusual for companies to contact you for business. Typically, though, you've done something to initiate that contact, and they're offering a legitimate service. Unsolicited contacts urging you to click a link, download software, or supply sensitive information are likely phishing expeditions. They're designed to get unsuspecting recipients to leak valuable data. They are continuously sent out because they continue to work. When Google conducted a study of phishing schemes in 2014, it found that while the lowest performers struggled to fool anyone, the most successful attempts succeeded nearly 45% of the time.

Pretexting are attacks that seek information on the basis of a legitimate or urgent need. It's unlikely that you will surrender valuable data to a complete stranger offering you a service you did not request. But when people believe there is a threat to their system, they develop an urgent need to calm the threat no matter the cost. This is the kind of thinking pretexting depends on.

Baiting describes offers of a good in exchange for an action or information. Ever get an email from a foreign dignitary asking you to supply your banking information so you can hold his money in exchange for a future payoff? If so, you've been baited.

Quid Pro Quo describes offers of a service in exchange for an action or information. While many people think of this as a legal term, it is also a Latin term that means "what for what" or "something given for something in return." It's much like baiting, except it puts a service rather than a good on the "hook."

Tailgating is the act of entering a facility directly behind someone who has used credentials for access. Make sure no one else is getting into your facilities without swiping a company name badge or entering the access code - a tailgater can cause trouble.

PROTECTING YOUR DATA

Hackers are looking for valuable data behind low-security barriers. Besides losing your clients trust, cyber attacks can have a wide range of consequences including threats to public safety, financial losses for you and your client, fraud and identity theft, lost time, and legal penalties and fines.

There are some simple steps you can take to make sure that you're firm is not an easy target.

GENERAL SECURITY POLICIES

- [ ] Lock down accounts after 10 failed login attempts
- [ ] Log users out of accounts after a period of inactivity
- [ ] Passwords must contain a capital and lowercase letter, a symbol, and a number
- [ ] Passwords must be changed at least quarterly
- [ ] Passwords may not be reused
- [ ] Maintain and Update your firewall
- [ ] Take cyber security classes to educate your firm

PROTECTING YOUR EMAIL

- [ ] Don’t open suspicious attachments or downloads
- [ ] Verify questionable emails with known sources
- [ ] Take extreme care with requests for sensitive information and develop strict procedures on how to handle this information
- [ ] Check that email addresses matches the text of the email and the organization’s normal email addresses
- [ ] Flag suspicious and forward it to your security team to deal with
- [ ] Don’t forward the email to anyone outside of your IT Team
- [ ] When in doubt, do not click any links in the email

PROTECT YOUR NETWORK

- ☐ Follow Company Policy
- ☐ Don’t Click on Suspicious links in emails
- ☐ Download only from trusted sites, and only after scanning them for viruses
- ☐ Make sure you see https in the address before transmitting any sensitive data
- ☐ Don’t connect systems to the network without notifying the security team
- ☐ Don’t bring hardware offsite without prior approval
  Report anything unusual to your security team

By following a few simple practices, you’ll make it much harder for criminals to get at your valuable information, and you’ll be able to keep your clients trust in your firm. In the day and age of technology, storing, keeping, and protecting information is of the utmost importance.

While you are busy tending to the needs of your clients and cases, there will always be someone, or group, out there working hard to break through barriers to steal your data. Stay alert.

CYBERLINK**ASP**

CYBERLINK**ASP**

While the detrimental effects of a cyberattack are more prominent in today's society than ever, the technological benefit of protecting your data is an essential for every law firm in practice. If you're itching to add an extra layer of security and accessibility to your firm, consider utilizing a free demo of our services.

Utilizing a cloud based desktop gives you the utmost security by hosting your data externally and keeping it monitored at all times. We firmly believe that our services speak for themself. Take advantage of our free 48 hour demo today to see what we can do for your firm.

www.CyberlinkASP.com