NYC BUSINESS SOLUTIONS

How-To Guide: Cyber Security

Content Provided by KALKI CONSULTING

Who needs cyber security?

NYC BUSINESS SOLUTIONS

Businesses that have, use, or support computers, smartphones, email, websites, social media, or cloud-based services.

Businesses that create, collect, store, or process any of the following types of information.

Intellectual property	Private information about your company's principals	Client names or records	Sensitive info e.g. merger or acquisition data
Payment info e.g. ACH, banking, or credit cards	Access to a business partner's web site	Patient medical records	Personally identifiable information

KALKI CONSULTING

Who is responsible for protecting me from cyber threats?

NYC BUSINESS SOLUTIONS

- **Within the company:**
  - Information Technology (could be outsourced)
  - Human Resources
  - Legal and Compliance (internal/external)
  - Finance
  - Public Relations
  - Internal Audit
  - Information Security Officer (for larger companies)

- **Outside the company:**
  - Federal and state authorities
  - Industry groups

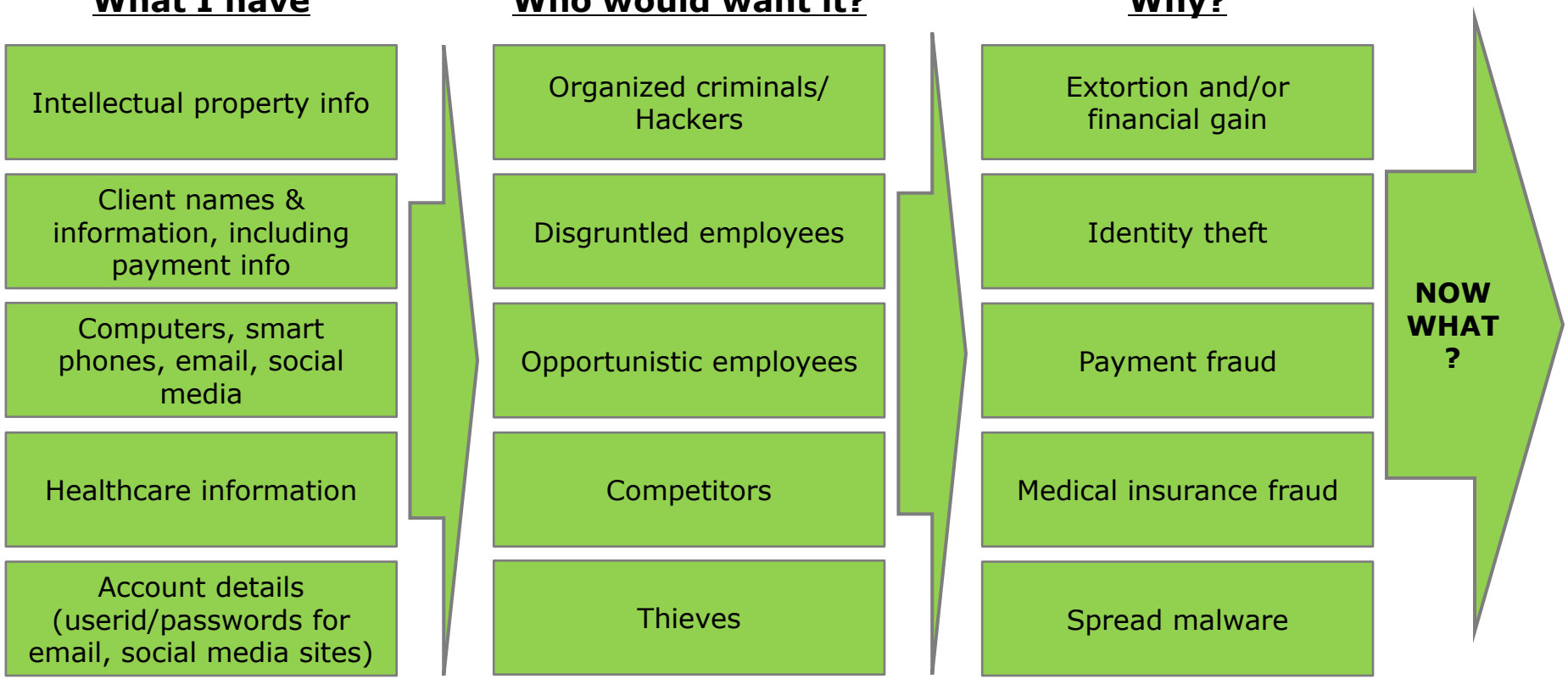
Ultimately the liability always will fall to the business owner and the risk will fall to investors, shareholders, employees, and clients.

KALKI CONSULTING

My business is small.
Why would anyone want my data?

NYC BUSINESS SOLUTIONS

Today cyber crime is now financially motivated and highly organized. Their tools are sophisticated. Cybercriminals, like bullies, prey on the easiest targets with the weakest security, such as small businesses.



KALKI CONSULTING

The impact of stolen data

NYC BUSINESS SOLUTIONS

While there are many impacts to cyber security, ultimately cyber incidents cost individuals, business owners, and the economy. In 2012 alone, cyber crime cost U.S. businesses $1 trillion.

What is the impact?

- Reputation & brand image issues
- Legal action & associated costs
- Violation of industry rules e.g. PCI-DSS
- Violation of federal laws e.g., HIPAA
- Loss of R&D time & money

SO WHAT?

Cyber security incidents cost

KALKI CONSULTING

How does cyber crime occur?

NYC BUSINESS SOLUTIONS

Small businesses rely on technology

Vulnerabilites are discovered for all systems

Unprotected technologies are exploited

"Hackers" create malicious code (malware) to discover unprotected technologies

Vulnerable systems are "hijacked" or "owned" by malware

Malware "hacks" email & social media accounts with weak passwords to spread itself

Malware collects sensitive information and sends it to criminals

Criminals use information to steal for financial gain

KALKI CONSULTING

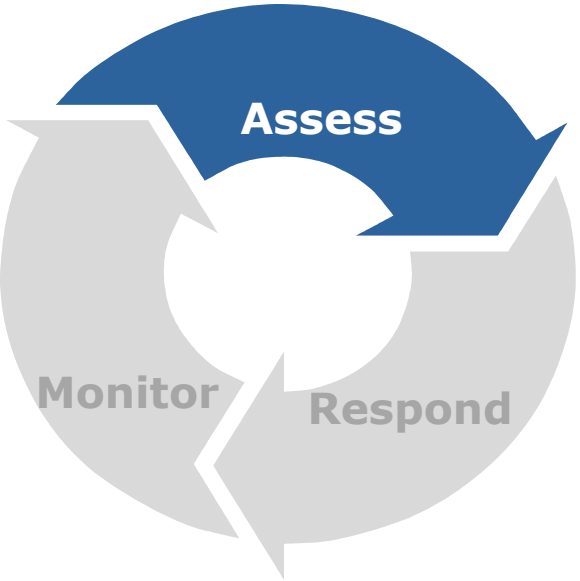
There's a problem. Now what?

There are 3 simple steps that a company can take to reduce the risk of cyber crime and incidents.

STEP ONE:

Conduct a cyber self-assessment. This will include:

- Documenting your information assets
- Identifying whether you have any regulatory or contractual obligations
- Measuring cyber security incident readiness
- Validating essential countermeasures

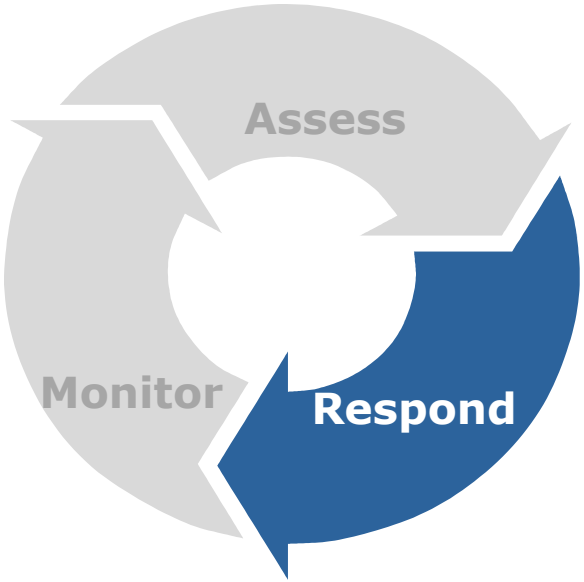


Cyber self-assessment considerations

- What data do you collect, store, process, or transfer?
- Who has access to it?
- What devices is/could it be stored on?
- What do you do if you lose it?
- If you lose it, do you need to let anyone know?
- What if an employee leaves your company?
- What if confidential data is emailed or uploaded to social media or other sites by mistake?
- How will you be able to assist the authorities in the event of a breach?

What happens after the assessment?

Once you have determined that risk exists, you need to be able to respond to it.



STEP TWO:

Cyber assessment response:

- Identify who will need access and how much access
- Develop a security and privacy policy that will protect your business in the event of an incident
- Educate everyone in your business to know what to do in the event of an incident
- Ensure that your technology environment has the basic countermeasures in place to respond to an incident

Cyber assessment response considerations

NYC BUSINESS SOLUTIONS

- Have you developed a security policy?
- Has the policy been communicated to all employees?
- Have your employees confirmed in writing that they understand the policies and the limitations?
- Do you have privacy policies that inform your customers how you protect their data?
- Have your employees been trained to respond to an incident such as loss or theft of a USB drive or laptop or a hack?
- Have you ensured that your technology environment has the basic countermeasures in place to respond to an incident, such as anti-virus on ALL machines (including MACs), encryption, and automated software updates and backups?

KALKI CONSULTING

How do you monitor for cyber incidents?

NYC BUSINESS SOLUTIONS

After assessing and responding, monitor for cyber incidents.

STEP THREE:
Once you understand where the risks are, you should consider policies and procedures to detect any:

- External malicious activity
- Unauthorized employee or partner access
- Problems with your technology

KALKI CONSULTING

Cyber monitoring considerations

With cyber security monitoring you should be able to:

- Watch for external access attempts to your network
- Determine if your cyber risks have changed
- Observe employees or contractors to ensure they are using the technologies and data as they should be
- Determine whether there are problems or vulnerabilities with your technology before an incident occurs

Cyber Security 101

IT is typically focused on operations, but cyber security is a dicipline that focuses on risk. The IT staff's top priority is NOT always security.

Cyber security is based on 3 tenets:

1. **Confidentiality**
   - Information is on a need-to-know basis
2. **Integrity**
   - Change or alteration of data must be authorized
3. **Availability**
   - Data must be there when you need it

Cyber security professionals believe in "Defense in Depth," meaning they never rely on one person or system to protect the business and the information it relies on to operate.

Simple CONFIDENTIALITY do's and don'ts

NYC BUSINESS SOLUTIONS

Confidentiality is:

Disclosing information on a need-to-know basis means:

DO:

- Ensure employee access is on a need-to-know basis
- Make sure everyone has their own account and password
- Keep passwords different and strong

and…

DON'T:

- Write your passwords down or share them with others
- Share company information with outsiders
- Assume emails and websites are secure because they say so

KALKI CONSULTING

Simple INTEGRITY do's and don'ts

NYC BUSINESS SOLUTIONS

Integrity is:

Making sure that any change of information is authorized means:

DO:

- Update and patch antivirus and system software regularly
- Encrypt devices that store your company's data
- Have a process for changing important data

and…

DON'T:

- Automatically download software because it's free
- Use file-sharing or peer-to-peer networks for free music
- Assume any technology device is immune from malware

KALKI CONSULTING

Simple AVAILABILITY do's and don'ts

NYC BUSINESS SOLUTIONS

Availability is:

Making sure that the data you need to run your business is there when you need it means:

DO:

- Have regular backups of data and keep them off site
- Consider computer locks, even in a shared office
- Plan for a natural disaster or technical incident

and…

DON'T:

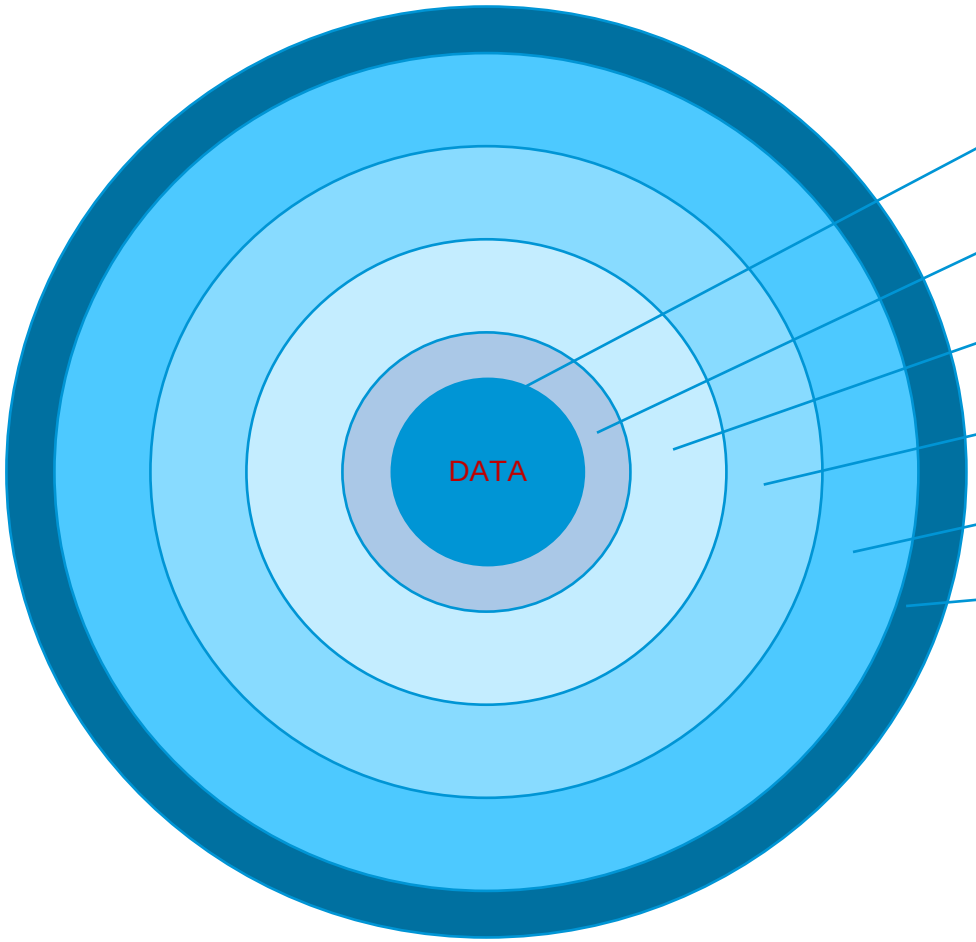
- Assume the backup works unless you test it regularly
- Assume the data is deleted once you get rid of a device
- Assume your IT/email provider will be able to protect you

KALKI CONSULTING

Defense in Depth 101

NYC BUSINESS SOLUTIONS

There are multiple layers that make up the technology we use. Defense in Depth requires security to be considered at every layer.



Database

Application

Operating system

Hardware

Network

Physical and environmental

KALKI CONSULTING

Kalki's SMB Cyber Self Assessment

NYC BUSINESS SOLUTIONS

Does the business owner care about…?	Losing money	Reputation & brand issues	Legal action	Industry rules	Violation of federal laws
	Yes / No	Yes / No	Yes / No	Yes / No	Yes / No
Does the business have…?	Banking or payment info	Intellectual property	Client names or records	Patient medical info	Sensitive info
	Yes / No	Yes / No	Yes / No	Yes / No	Yes / No
Do you protect yourself with…?	Security policy	Employee training	Incident response plan	Security technology	Physical security
	Yes / No	Yes / No	Yes / No	Yes / No	Yes / No

If you answered "yes" to any of the questions above you should:

- Work with a qualified Cyber Security professional to assess your risk
- Have a set of documents that will protect you if you are audited
- Implement policies and procedures that allow you to detect and respond to incidents
- Not rely on a singe technology or software to save you!

KALKI CONSULTING

Kalki Consulting

NYC BUSINESS SOLUTIONS

KALKI CONSULTING

Founded & based in New York, Kalki Consulting LLC provides cyber security services to small, medium and enterprise companies with independent cyber assessment, response and monitoring offerings.

Kalki is committed to helping clients understand and manage their regulatory compliance and cyber exposure to a security incident.

For additional information go to:

Web:	http://www.kalkiconsulting.com
Twitter:	@kalkiconsulting
Facebook:	https://www.facebook.com/KalkiConsulting
Phone:	1-855-GO-KALKI (1-855-465-2554)

KALKI CONSULTING