360°

of IT Compliance FOR BUSINESS

Table of Contents

Part One

Evaluating Your Network Environment

Prepared by:

SymQuest®
A KONICA MINOLTA COMPANY

360° of IT Compliance – A Guidebook

Is your business fully compliant with the latest IT best practices and regulations? In this guidebook we will give you a few tools to begin the process of evaluating your compliance needs. Should you run into questions we would be happy to assist you. Contact us at:

SymQuest Group, Inc.
(800)-374-9900
info@symQuest.com

Downs Rachlin Martin
(802)-863-2375
info@drm.com

Layered Security Model

When evaluating your internal security protocol it's helpful to use a *Layered Security Model*. This model begins with the internet and ends with the employee. Follow along with the flow of this model below.

Internet 

Email Filtering

The filtering of spam and virus infected email should occur outside your firewall. Not only does this reduce the amount of traffic on your internet connection, it ensures that email based malicious code never enters your network. Additionally, you can set up your firewall to only accept email from a known source, your email filtering service.

Web Filtering

End users should be prevented from accessing websites that are known malicious sites. This is not simply a matter of making sure that users are not wasting time or exhibiting questionable taste. This is about real threats to your network.

Firewall

This is the *cyber front door* to your organization. Just like your physical front door it should be locked down and only authorized traffic should be allowed through.

Network Access Control/Wireless Security

Only authorized devices should be allowed to connect to your network. In the case of wireless devices, those devices should be limited to accessing only those resources they are supposed to. For example, wireless guest access should only allow users to get to the Internet but not have any visibility to internal network resources.

Network Security Monitoring

Just like you might have motion sensors in your office to detect suspicious movements when you are not there, you might have monitoring on your network to detect suspicious traffic. Similar to your physical security, this may be a service provided by a third party.

Operating System Security Patches

Operating Systems (OS) are constantly being updated with security patches as vulnerabilities are discovered. Failure to apply these patches and reboot systems regularly leaves an organization vulnerable to exploits by hackers. Once a patch is released the entire hacker community is aware of the vulnerability.

Anti Virus/Anti-Malware Updates

New Viruses are deployed every day. Your antivirus and anti-malware software needs to be kept up to date. If your AV/AM software has not been informed of the existence of a new virus through an update, it cannot detect it.

Application Security patches

Similar to an OS, applications are updated regularly to address vulnerabilities discovered. Something as simple as opening a PDF file can put an organization at risk if the application is not patched.

Employee Education

The last line of defense is the *Employee*. Most major security breaches involve an employee action that enabled hackers to gain access to the system. Employees must be educated on network security best practices. Your employees should be your *"human firewall"*.

Employee "Human Firewall"

Top 10 Things Every Employee Should Know About Network Security

1. **Never divulge your password…*to anyone*.** Nobody else needs to know your password, even system administrators. If they need to log in as you to recreate a problem they can change your password temporarily and you can reset it later. Administrators should never ask users for their passwords or keep lists of end user passwords. This circumvents potential for an audit trail should it be needed down the line.
2. **Lock your screen when you are away from you PC.** When you step away from your desk make sure someone cannot sit at your desk and access the corporate network. That person can do something as silly as crafting a nasty email to the company president or something as devious as stealing confidential information. On a Windows 7 PC hit the Windows key and the letter "L" as a quick way to lock your computer.
3. **Scrutinize the email addresses of senders.** "Spear phishing" email scams are real. These are directed attempts to dupe specific individuals into executing a transaction based on familiarities. The email appears to be from someone you know or claims to know you through a common acquaintance. These can be very convincing but there are usually clues that it is a phishing scam. Does the email come from a domain that matches the sender's organization? Is the domain spelled correctly?
4. **Do not open emails from people you do not know.** We all get emails from people we don't know every day so this one is a bit difficult. However, if you set up your email client to preview the first couple of lines of the email you can usually get a sense as to whether it is a legitimate communication.
5. **Be careful clicking on hyperlinks embedded in emails.** Another trap in the "spear phishing" scam is to trick the user into clicking on a link in an email that will take them to a malicious website that will install viruses or malware. Or perhaps present itself as a legitimate website and ask the user to enter personal information. The link in the email may say Bank of America; however, when you hover your mouse over the link it may show www (dot) reallybadsite (dot) com.
6. **Use a PIN to access your smartphone or tablet.** Smartphones and tablets are very portable and convenient. They may also contain a lot of sensitive data. Many smartphone apps store your credentials so you don't have to enter them each time you launch their app.

Make sure that convenience is not provided to others that may get a hold of your phone Never leave your laptop, smartphone, or tablet unattended in a public space.

7. **Never leave your laptop, smartphone, or tablet unattended in a public space.** This best practice is pretty obvious but leaving devices unattended does occur. Encourage your employees to keep track of their work devices. You may also consider best practices for storing laptops when not in use.
8. **Report the loss of a laptop, smartphone, or tablet immediately.** Depending on the industry and the type of data stored on the device there may be serious consequences to the organization associated with the loss or theft of a device. There are reporting guidelines for such instances. Also, mobile devices should be encrypted to ensure the data can't be retrieved by non-authorized persons. Likewise, IT departments should have the ability to remotely wipe personal devices that are connected to the corporate network. The sooner the risk is mitigated the better.
9. **Be wary of public wifi.** Typically, public wifi is exactly that…public. Information sent over the airwaves can be "seen" by others. Avoid sending confidential information (credit card info, corporate email, Social Security numbers, etc.) over public wifi unless you know you have a secure link (encrypted).
10. **Report any security incident (email scam, suspicious behavior, etc...) to your IT administrator immediately.** Even if you think you have made a mistake and violated one of the rules above, report it to your administrator rather than ignore it or hope it goes away. The entire organization should be aware of any active scams.

IT Perception Survey

Take this assessment to determine where your business IT needs are. Hint: you will want to land mostly in the green. If you find you're coming up red – give SymQuest a call today. We can help bring you back to green.

	Reliable	Somewhat Reliable	Unreliable
IT Facets – Level of Reliability			
IT Personnel			
Environmental Requirements			
Daily Support For End Users			
Hardware Scalability Issues			
Documented Plan for Business Continuity			
Fault Tolerance/Redundancy			
Data Backup: Verify and Recovery			
Maintaining Regulatory Compliance			
Regulatory Compliance Audits			
Maintaining System Security			
Applying Security Updates			
Intrusion Protection			
Protection from Internet Vulnerabilities			
Virus and Malware Infections			
Software License Tracking			
Common GUI Across the Network			
Component Replacements and Upgrades			
Hardware Repairs			
Hardware Warranty Tracking			
Integration of New Hardware and Software			
Additional Investments for Secure Remote Access			
Configuration of Print Drivers			

Part Two

Cyber Insurance and Legality

Prepared by:

DRM | Downs Rachlin Martin PLLC

Business Sense · Legal Ingenuity

DRM Downs Rachlin Martin PLLC

Business Sense·Legal Ingenuity

Five Notes
On Data Breaches:

Matthew S. Borick
Downs Rachlin Martin PLLC
mborick@drm.com

Important notes on data breaches.

1. **The "numbers" are staggering:**
   - 60,000 new pieces of malware created each day
   - 3 to 4 breaches in the U.S. each day
   - Average cost of a breach = $6.5 million
2. **Complete prevention is virtually impossible, so the focus must be on minimizing risk and impact.**
3. **Data breaches have a before, during, and after:**
   - Before = prepare adequately
   - During = detect early
   - After = respond effectively

   The "before" is the most important part!
4. **Breach notification obligations may extend far beyond the state in which your business is physically located.**
5. **Successful data security requires 100% commitment, and a little common sense.**

drm.com

DRM Downs Rachlin Martin PLLC
Business Sense · Legal Ingenuity

Privacy + Data Security For Cyber Risks:

Matt Borick
Downs Rachlin Martin PLLC
mborick@drm.com

Step 1 Identify "personally identifiable information" (PII)

PII is information that is directly about, or can be traced back or linked to, any individual's person. Examples:

- Name
- Address
- Personal phone number
- Personal fax number
- Date of birth
- Social Security Number
- Age
- Gender
- Personal e-mail address
- Passwords
- Physical characteristics
- Driver's license number
- Non-driver ID card number
- Financial account number
- Service account number (utility, cable, etc.)
- Credit or debit card number
- Financial account access code/PIN
- License plate number
- Mother's maiden name
- Health/medical information
- Purchasing behavior information
- Benefits information
- Education records
- Salary information
- Employment records
- Military records
- Law enforcement/arrest/conviction records
- Medical device identifiers (pacemaker IDs, hearing aid IDs, insulin pumps, etc.)
- Marital status
- Family information
- Religious views information
- Political views information
- Sexual preferences
- Association membership records (e.g., union)
- Biometric identifiers

Step 2 Identify the privacy and data security goals and objectives of your organization

- Minimize theft of, loss of, misuse of, inadvertent disclosure of, or unauthorized access to PII
- Protect valuable trade secrets and confidential data
- Maintain competitive advantage
- Establish positive business image
- Establish employer/customer/stakeholder confidence
- Minimize risk of regulatory penalties and civil/criminal liability

Step 3 Assess risks by identifying PII that you collect, store, use, process, share, transmit, and/or dispose of; identify "data flow" into, through, and out of your organization

What hardware and software assets do you have? _____

_____

What PII do you collect, use, store, etc., in your business? _____

_____

For what purpose do you collect, store, use, etc., PII?_____

Do you have a legitimate business need for all the PII you collect, store, use etc., or do you need to go on a "data diet"?

☐ Legitimate business need ☐ "Data Diet"—reduce, collection, storage, etc.

From whom do you collect or obtain PII? (COPPA triggered if from children under 13)

_____

_____

In what states or countries are these people located?_____

In what form do you collect PII (e.g., physical files, electronic files and data, etc.)?

☐ Physical (paper) files ☐ Databases

☐ Electronic files ☐ Other_____

How do you collect PII?

☐ Forms ☐ Collect on purchases

☐ Surveys ☐ Purchase data

☐ Information requests ☐ Hidden website cookies (NOTE: Failure to disclose may constitute "unfair practice")

☐ Sign-ups/applications

DRM Downs Rachlin Martin PLLC
Business Sense·Legal Ingenuity

Where and how do you store PII?

- ☐ Computers (desktop, laptop, tablet, server)
  - ☐ Office computers
  - ☐ Home computers
- ☐ External drives and disks
- ☐ Hard copy files (on-site and off-site)
- ☐ Cell phones (voicemail, e-mail, texts, social media)
- ☐ Telephones (voicemail)
- ☐ Digital copiers, printers, fax machines, multi-function machines
- ☐ Other_____

Do your employees have laptops, tablets, or other portable computers that contain PII? Identify all.

_____

Do you keep copies or backups of PII? Identify how. _____

_____

Who has access to PII you collect or store, and how can they access it?_____

_____

Who needs access to the PII you collect or store? _____

_____

What (e.g., automated systems) has access to PII?_____

_____

Do any people with access work remotely (home, on travel, job site, etc.)?_____

How do you process and use PII? _____

_____

In what states do you store, process, etc. PII?_____

In what countries do you store, process, etc., PII? _____

_____

With whom do you share PII?

- ☐ Internal only
- ☐ Third Parties
  - ☐ Customers
  - ☐ Vendors
  - ☐ Professional service organizations (legal, accounting, financial, consulting, etc.)
  - ☐ Others

How (by what means) do you share or transmit PII?

- ☐ Physical copy exchange
- ☐ Fax
- ☐ E-mail
  - ☐ Secure
  - ☐ Unsecure
- ☐ FTP servers
- ☐ Cloud (Dropbox, etc.)

What do you do with PII when you no longer need it?_____

_____

How do you dispose of PII? _____

_____

How do you track the use, transmission, disposal, etc., of PII in your organization?

_____

_____

Who poses a threat to misuse the PII you collect or store?

- ☐ Internal (employees)
- ☐ External (business partners, contractors, vendors, customers, hackers, etc.)

Under what circumstances do you permit PII to be disclosed?

- ☐ Consent required (express or implied)
- ☐ Consent not required

Step 4 Manage risks by identifying what controls you have in place to protect PII

What people are in charge of privacy/data security and are accountable for it in your organization?

- ☐ Chief Technology Officer
- ☐ Chief Information Officer
- ☐ Chief Privacy Officer
- ☐ Chief Compliance Officer
- ☐ Office Manager
- ☐ Security Officer
- ☐ IT Manager/Department
- ☐ HR
- ☐ Legal
- ☐ Risk Management Specialist
- ☐ Others
- ☐ "Steering committee" composed of senior leadership from across the organization (legal, compliance, enterprise infrastructure, IT and security, human resources, marketing, public relations, procurement, business units)

DRM Downs Rachlin Martin PLLC
Business Sense·Legal Ingenuity

What do these people do to perform these roles effectively?_____

_____

Who in your organization decides what is PII and what is not? _____

_____

Who in your organization assures that PII is accurate? _____

_____

What technological safeguards do you have in place to protect PII?

☐ Unique logins
☐ Passwords (including separate, unique passwords for servers)

- ☐ Hard to guess (impersonal, mix of characters, etc.)
- ☐ Frequently changed
- ☐ Different passwords for different things
- ☐ No use of default passwords
- ☐ No "remembering" of passwords by computers, devices, etc.

☐ Automatic "locking" of devices when unattended or not in use
☐ Authentication of people using and accessing PII
☐ Encryption
☐ Secure connections [secure sockets layer (SSL), etc.]
☐ Network segregated into separate security domains (unique access credentials for each)
☐ Firewalls
☐ Electronic monitoring of PII traffic in and out
☐ Intrusion detection systems
☐ Automated monitoring/analytics/response capabilities
☐ Caller ID phones
☐ Central log files of security-related information (physical and electronic)
☐ Centralized control over settings on individual devices containing PII
☐ Clawbacks/e-mail retrieval
☐ Anti-virus
☐ Spyware protection
☐ Properly configured software
☐ Known/reputable software
☐ Software security patches
Make sure to install all patches and updates to operating systems and applications in order to address vulnerabilities.
☐ Secure wireless networks

☐ Permanent/non-recoverable/secure deletion of electronic files

☐ Prevention of former employees accessing data (cancel passwords, etc.)

☐ Redaction on electronic documents

☐ Remote "kill switch" that disables lost/stolen laptops, computers, cell phones, etc.

☐ Use of reputable vendors/consultants for your IT systems

Make sure any access rights are appropriate (limited to "as needed").

Make sure to change access credentials after their work is finished.

☐ For service accounts (user credential/account used to run server or a process on a server)

Make sure to follow best practices.

Make sure not to leave any default passwords in place.

What administrative/operational/procedural safeguards do you have in place to protect PII?

☐ Comprehensive data security policy

Purpose _____

Scope _____

Team _____

Role and responsibilities _____

Compliance _____

Procedures _____

Revisions/updates _____

☐ Privacy Policy

Components

Information collected _____

_____

Purpose for collection _____

_____

Use of information _____

_____

Person's access to his/her own information_____

_____

DRM Downs Rachlin Martin PLLC
Business Sense·Legal Ingenuity

Opt–outs/choice_____
_____

Disclosure of security_____
_____

Is the policy open and communicated well? _____

Is the policy strictly followed?_____

☐ Rules/policies for employees who have access to PII

☐ Use restrictions for work e-mail, computers, internet, etc:

- ☐ Avoid e-mailing PII in plain text
- ☐ Avoid e-mailing PII to personal e-mail
- ☐ Avoid using unprotected attachments
- ☐ Avoid opening suspicious attachments or clicking on suspicious web links ("spear phishing" or "pharming")
- ☐ Avoid using open or unencrypted wireless networks

☐ Security guidelines for laptops and other portable devices when taken offsite

☐ "BYOD" (bring your own device) policies to address personal devices that are used for business purposes

☐ Employee intake procedures

- ☐ Confidentiality agreements
- ☐ Reference/background checks in hiring process

☐ Separation of employee duties (no one person does it all)

☐ Posted "reminders" in areas where PII is used or stored

☐ Communication procedures to facilitate internal reporting of incidents

☐ Social media policies

☐ Rules and minimum standards you set for third parties with whom you share or use PII

☐ Contractor, vendor, service provider, etc., privacy and security policies

☐ Contracts with third parties with whom you share or use PII

☐ Provisions governing data security practices:

- ☐ Written security program
- ☐ Compliance with applicable laws
- ☐ Restrictions on use of data
- ☐ Indemnification/hold harmless provisions
- ☐ Privacy policy provisions
- ☐ Prompt notice to you of potential incidents

- ☐ Safe return/destruction of information
- ☐ Insurance provisions

☐ Education, training, and other means to increase awareness and understanding, ensure compliance, and solidify response protocols

- ☐ Reinforce that security is a top priority for all
- ☐ Create a "risk aware" culture

☐ Periodic internal testing for vulnerabilities

☐ Regular review of expert websites (e.g., www.sans.org) and other sites for information on new vulnerabilities

☐ Collect, store, use, etc., only the PII you need for only as long as you need

☐ Tracking and implementing of opt-out and opt-in preferences

☐ Monitoring of who has keys and other access tools (including retrieval at termination)

☐ Management endorsement and buy-in of privacy governance framework

What physical safeguards do you have in place to protect PII?

- ☐ Locked rooms, cabinets, file drawers, etc.
- ☐ Physical lockdown on portable computers
- ☐ Controlled access to locations where PII is kept or used
- ☐ Shredding of paper records
- ☐ Prevention of former employees accessing (get keys, etc.)
- ☐ Redaction on paper documents
- ☐ Fax machines in secure, supervised areas
- ☐ Heightened attention to small devices (e.g., thumb drives)
- ☐ Other _____

How up-to-date are your safeguards? _____

_____

Step 5

Comply by identifying what laws, regulations, guidelines, standards, etc., you are required to follow or should follow with respect to PII

Who in your organization monitors for compliance? _____

_____

What laws, rules, standards, guidelines, etc. apply to you? [NOTE: This can depend (in part) upon the residence of people whose data you have] _____

_____

_____

Some Examples:

- HIPAA (Privacy Rule, Security Rule, Omnibus Rule)
- HITECH
- Health Insurance Exchange Rules (45 C.F.R. § 155.260)
- GLB Act And Safeguards
- COPPA
- Privacy Act
- Security Breach Notice Acts (State)
- State Data Security Laws
- FTC Act And Fair Information Practices
- Red Flags Rule
- CFAA
- EPCA
- SCA
- ISO27001 Security Standards
- AICPA Generally Accepted Privacy Principles (GAPP)
- Payment Card Industry (PCI) Standards
- Self-Regulatory Initiatives
- Fair Credit Reporting Act
- Fair And Accurate Credit Transactions (FACT) Act
- Trade Association Security Guidelines
- Password Privacy Laws
- Common Law (Judicial Decisions)
- Mobile Marketing Association Guidelines
- Digital Advertising Alliance Form Of Notice
- Video Privacy Protection Act
- NIST Cybersecurity Framework
- FISMA Self-Assessment
- Many Others….

What governing bodies enforce the privacy rules applicable to you?

- ☐ FTC
- ☐ Other federal agencies (HHS, SEC, FCC, etc.)
- ☐ State attorney general
- ☐ State agency
- ☐ Industry association
- ☐ Others

Step 6

Enhance response preparedness by identifying what plans and protections you have in place to deal with a breach

How will you know if there has been unauthorized activity? _____

_____

Who is on your organization's response team?

Internal

- ☐ Executives/managers
- ☐ IT
- ☐ Legal
- ☐ Financial
- ☐ Customer Service
- ☐ HR
- ☐ PR
- ☐ Other _____

DRM Downs Rachlin Martin PLLC
Business Sense·Legal Ingenuity

External

- ☐ Attorneys
- ☐ Forensic investigators
- ☐ Consultants
- ☐ Law enforcement
- ☐ Other _____

Are roles and responsibilities well defined?_____
_____

What preparedness/response plans do you have in place? _____
_____

What corrective action and remediation plans do you have in place?_____
_____

What notice protocols and procedures do you have in place?_____
_____

Do you have cyber-risk insurance?

- ☐ First-party coverage (damage to you)
- ☐ Third-party coverage (damage to others)

drm.com

DRM Downs Rachlin Martin PLLC
Business Sense·Legal Ingenuity

Road Map to the Vermont Security Breach Notice Act (9 V.S.A § 2435)

Part 1 – Does the Act Apply?

STEP 1
Are you a data collector?

If yes, continue to Step 2
If no, the Act does not apply

You are a data collector if, for any purpose and by any means, you:

- Handle
- Collect
- Disseminate, or
- Otherwise deal with…

…Consumers' (Vermont residents) **"personally identifiable information" ("PII")** that is (a) not publicly available and (b) not encrypted, redacted or otherwise protected from unauthorized view or use.

PII includes a person's first name (or initial) and last name **in combination with** any of these:

- Social Security number
- Driver's license number
- Non-driver ID card number
- Financial account number
- Credit or debit card number
- Financial account access code (e.g., PIN)

STEP 2
Do you own or license computerized data containing PII? Do you maintain or possess any records or computerized data containing PII that you don't own or license?

If yes to any, continue to Step 3
If no, the Act does not apply

STEP 3 Have you had a "security breach"?

If yes, continue to Step 4
If no, the Act does not apply

A security breach is defined as:

An unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer's PII.

To determine if you've had a security breach, you may consider factors such as:

- Whether the data is in the physical possession and control of an unauthorized person (e.g. lost/stolen computer or device)
- Whether the data has been downloaded or copied
- Whether the data was used by an unauthorized person (e.g., instances of identity theft have been reported)
- Whether the data has been made public.

NOTE: A "security breach" does not include an unauthorized acquisition of PII by your employee or someone acting on your behalf, as long as:

- The acquisition was in good faith
- The acquisition was for a legitimate purpose of yours
- The PII is not used for a purpose unrelated to your business, and
- The PII is not subject to further unauthorized disclosure.

Road Map to the Vermont Security Breach Notice Act (9 V.S.A § 2435)

Part 2 – What Notice Requirements Apply?

STEP 4

Is there a reasonable possibility of misuse of any PII acquired in the security breach?

If no

If yes, continue to Step 5

You don't need to provide notices required by Section 2435(b),

But:

- If you are licensed or registered with the Department of Financial Regulation under Titles 8 or 9 of the VT Statutes, you must inform the Department that you have had a security breach but have determined that misuse of PII is not reasonably possible, and must provide a detailed explanation for your determination. Otherwise, you must provide this information to the VT Attorney General.
- If you later learn that misuse of PII has occurred or is occurring, you must provide the notices required by Section 2435(b).

STEP 5

You must provide the notices required by the Act.

If you own or license computerized data containing PII:

Notify affected **consumers** as quickly as possible, **but no later than 45 days** after you discover or are notified of the breach.

NOTE: You may delay the required notice if you are requested to do so by a law enforcement agency.

The notice to consumers may be made directly via written, telephonic (but not prerecorded) or electronic means. If you can demonstrate that the cost of providing notice would exceed $5,000 or the number of affected consumers exceeds 5,000, or if you don't have sufficient contact information, you may provide "substitute" notice through a conspicuous posting on your website **and** notification to major media.

The notice to consumers must be **clear and conspicuous**, and must include the following, if known:

- A description of the breach including the approximate date and the type of PII that was subject to the breach;
- A description of your general actions to protect the PII from further breaches;
- A telephone number consumers may call for further information and assistance; and
- Advice directing consumers to remain vigilant by reviewing account statements and monitoring free credit reports.

If you maintain or possess any records or computerized data containing PII that you don't own or license:

Notify the **owner or licensee** of the PII **immediately** after you discover or are notified of the security breach. (The owner or licensee must provide the notice described earlier.)

Other required notices

Preliminary notice to Vermont agencies:

- If you are licensed or registered with the Department of Financial Regulation under Titles 8 or 9 of the VT Statutes, notify the Department of the breach. Otherwise, notify the VT Attorney General.
- The notice must include date of the breach, date of discovery of the breach, description of the breach (including number of Vermont consumers affected, if known), and a copy of the notice provided to consumers. If you don't yet know the date of the breach, you must provide that to the Department or Attorney General as soon as it is known.
- Make the notice to the Department or Attorney General **within 14 business days** after you discover the breach, or at the same time notice of the breach is provided to consumers, **whichever is sooner.** (EXCEPTION: In one circumstance you must notify the Attorney General before notifying consumers.)

Notice to credit reporting agencies:

- If you need to provide notice to more than 1,000 consumers for a breach, you must also promptly notify all national consumer credit reporting agencies (Equifax, Experian, and TransUnion) of the timing, distribution and content of the consumer notice.

DRM Downs Rachlin Martin PLLC
Business Sense·Legal Ingenuity

Tips for Purchasing Insurance For Cyber Risks:

Bruce Palmer, Director
Downs Rachlin Martin PLLC
bpalmer@drm.com

Tip 1

Determine your existing coverage first.

What you have:

- You may already have some coverage. For example, professionals handling confidential or private information may have professional liability or errors and omissions policies that cover breach of confidentiality or privacy through a cyber attack. Crime or fiduciary liability or other policies also may provide coverage limited to a particular context or events.

Watch for exclusions:

- Many existing policy forms simply say nothing about cyber risks and liability. The insurance industry is adding privacy and data breach exclusions to many policy forms. Comprehensive general liability policies, for example, will now often exclude data breach liability risks.

Policy Supplements:

- A supplement to your policy may be present or available for an additional premium. Some companies offer "bolt on" endorsements to small business owners' policies. These products are less comprehensive than stand-alone coverage, but may suffice for a smaller business that does not handle extensive personal data or sensitive information.

Cyber Risk:

- When in doubt, do not assume you are covered. The trend increasingly is to funnel all cyber risks into the fast growing market for cyber risk policies.

Tip 2

Understand the market.

Lack of Standardization:

- Policy language is not standardized. Many different companies are offering products that vary significantly even in the basic grants of coverage. It may be some time before policy language gains more uniformity, and this is both a risk and an opportunity, as some coverage features and limits may be negotiable.

Evolving Coverage Boundaries:

- Cyber risk coverage is a fast growing market, and the contours of coverage are not yet fully tested in courts or through claims and loss history. Premiums vary by business type and resulting risk profiles and may fluctuate.

Establishing Precedent:

- As more cases are decided by courts and more claims data is examined, underwriters will gain a better perspective on coverage and policy language and pricing may start becoming more standardized.

Scrutinize Carefully:

- Look hard at what you are buying. Both first party coverage for your own losses and third party coverage for liabilities to others are offered, and you can purchase coverage and limits that best fit your industry, business model and size.

Bundling:

- Bundling of coverage and package policies with less flexibility of choice is also a growing trend.

Tip 3 — Consider how these provisions may affect the extent of coverage.

Response, notification and remedial expenses:

- Particularly for companies that handle a large amount of customers' or clients' personal information, look carefully at what is covered with respect to forensic investigation, data breach notification and credit monitoring. These can be some of the largest expense obligations arising out of a breach of your data security.

Limits, sub limits and aggregates limits:

- You should carefully consider the amounts provided for categories of expense or liability. Purchase enough to meet your needs, but not so much that you pay excessive premium. Benchmarking can help, but is no substitute for a rigorous examination of your own particular business practices and potential liabilities.

Exclusions:

- These vary and can have a significant impact on the coverage provided. Even small nuances of language can be exploited to argue that a claim is within or outside of the coverage provided. Seek more than one quote and compare the coverages carefully with a qualified insurance professional or attorney.

Application Accuracy:

- Applications are detailed and will inquire about your policies and the state of compliance of your information systems with industry standards. Coverage can be rescinded (voided after the fact) if a representation is false, material to the risk and relied upon by the insurer, even after coverage is bound and a loss has occurred. Pay close attention to the accuracy of your application.

Use of Data by Vendors:

- Third party liability coverage for breaches caused by companies storing, using or accessing your data is not provided under all policies. If you use the cloud or regularly entrust data to vendors in your business, be sure they are covered, through the vendor's policy naming you as an additional insured or your own coverage.

Fines and Penalties:

- Coverage for regulatory or statutory fines or penalties varies significantly among policies. Determine up front whether the policy will cover such fines or penalties, not after the fact.

Retroactive dates:

- You may have had a breach already that you will not discover for some time. A retroactive date provision will limit coverage to events happening after a certain date which may be as late as the inception of the coverage under your initial policy. Negotiate if possible for an earlier date.

Value Added Services:

- Finally, consider the value added services provided under some programs. Some companies may offer free or reduced price risk management services or periodic systems audits or penetration testing, which can be a valuable resource to your IT team and improve the overall security of your systems.

drm.com

DRM Downs Rachlin Martin PLLC
Business Sense·Legal Ingenuity

Five Step
Incident Response Plan:

Joseph L. Choquette, III, Public and Governmental Affairs
Downs Rachlin Martin PLLC
jchoquette@drm.com

The 5 step plan.

1. **Contain the crisis.**
   - Stop the damage, reduce the risk
2. **Assemble the incident management team.**
   - Identified in advance
3. **Assess the situation and identify impacts.**
   - Get all of the facts of the breach
   - Consider effected audiences
4. **Prepare a communication plan.**
   - Designate one spokesperson and advise employees
   - Prepare immediate holding statement
   - Prepare and refine talking points
   - Identify how to communicate and to whom
5. **Execute.**
   - Email, press release, letter to clients, website, news conference, media conference call, social media

drm.com

DRM Downs Rachlin Martin
Business Sense·Legal Ingen

Reputation Management
Basic Tool Kit:

Joseph L. Choquette, III, Public and Governmental Affairs
Downs Rachlin Martin PLLC
jchoquette@drm.com

The basic tool kit.

Contact Lists

- Crisis or incident team: Executive, Finance, HR, PR
- Consultant list and contact names
- Employees, vendors, customers
- News media

Communication Plan

- Written plan
- Holding statement
- Talking points
- Communication to staff, customers, clients
- If Asked – Q & A
- Draft Release

SymQuest®
A KONICA MINOLTA COMPANY

(800) 374-9900 | **SymQuest.com**

DRM | Downs Rachlin Martin PLLC
Business Sense·Legal Ingenuity

(802) 863-2375 | **drm.com**