PRO BONO™
PARTNERSHIP / ATLANTA

This article presents general guidelines for Georgia nonprofit organizations as of the date written and should not be construed as legal advice. Always consult an attorney to address your particular situation.

MANAGING CYBERSECURITY RISK FOR NONPROFITS

By Michael Ridgway Jones, General Counsel, Riskonnect, Inc.

CYBERSECURITY: SHOULD YOU BE CONCERNED?

- Does your organization collect or store **personal information** or **sensitive proprietary information?**
- Does your organization host a **public website** that interacts with individuals and collects or stores their personal information?
- Does your organization use a **third-party vendor** to manage your database, provide user support or fulfill any user requests?
- Would your organization be **negatively impacted** by a security breach or ransomware attack?
- Does your staff use **their own devices** for work or routinely **work remotely**?

If the answer to any of the above questions is “yes”, here are some things you can do to protect your organization and mitigate potential risks of a security incident:

- ***Inventory and Map Your Data***: You must know **what** data you touch, **where** it comes from, **where** it goes and **how long** you keep it. Particularly important here is the question of **where** the individuals who are the subjects of the personal data reside, as this will drive notification requirements if there is a data breach.
- ***Review Data Security Controls***: If you’re trying to put controls in place after the fact, it’s too late! Review your current controls and processes **now**, identify any gaps and take steps to remediate them. Tools like multi-factor authentication and firewall controls (among others) are key.
- ***Implement and/or Evaluate an Incident Response Plan***: An incident response plan is key, and no business is too small to have one. Again, the last thing you want to do when you’re hit with a security incident is to be trying to come up with a plan on the fly. You need to have one **now**. There are many standard-setting organizations out there that can provide you with guidance and best practices, and consultants and outside counsel abound to advise on implementation.
- ***Vendor Management Protocols***: As some recent (and not-so-recent) data breaches have shown, sometimes the weakest link in your security posture is a third (or fourth) party which may not have the same controls in place as you do. Having a process in place for screening and monitoring vendors (even ones that might not seem that mission critical) is key.
- ***Cyber Insurance***: If your business accesses or uses personal data, you need to talk to an insurance professional about possibly buying coverage to protect against losses from a security event.

CYBER INSURANCE: THE PROBLEM

Most standard commercial general liability (CGL) insurance policies **do not cover** liability for cybersecurity issues. Standard CGL policies cover such items as bodily injury, property damage, and even advertising injury. However, “property damage” is usually interpreted to mean damage to **tangible** property, and electronic data is typically excluded as **not** tangible property.

CYBER INSURANCE: THE SOLUTION

Cyber insurance can address gaps in coverage that may arise under traditional commercial insurance policies.

KEY QUESTIONS

- How much insurance do you need and how much can you afford?
  - The cost is usually based on the number of records you have and the type of information you collect
  - The cost per record rises as the number of records increases
- What are the deductibles? Are there any limits or sub-limits?
- Would the policy provide coverage in excess of any other insurance your organization may carry?
- What territory is covered? Is coverage global or limited to the U.S.?
- What are your unique risks? For example, do you store credit card data? Health-related information?
- What should trigger coverage under the policy? An intentional cyberattack only? Or any breach, including one caused by negligence or unintentional error?
- What is the insurer's response time in case of a data breach? Does it offer a 24/7/365 data breach hotline?
- Will your insurer increase your premium if you make a claim?
- What periods are covered under the policy? Some incidents aren't discovered until years later. (To protect against a potential gap in coverage, try to negotiate **retroactive coverage**.)
- What does your policy **exclude**? Typical exclusions are
  - Bodily injury
  - Property damage
  - Employment practices
  - Pollution
  - Antitrust violations
  - ERISA violations
  - Telephone Consumer Protection Act (e.g., robocalling, junk fax) violations
  - Directors' and officers' intentional acts
  - Unlawfully collecting personal or other non-public information
  - Negligent information security practices (e.g., failing to install software patches for known vulnerabilities)
- Will your insurer defend your organization in a lawsuit or regulatory investigation (the insurer's "duty to defend")?
  - What **additional services** does the provider offer? Examples: audits, penetration testing, incident response plan assessments
- What are your audit and compliance obligations under the policy?

HOW TO ASSESS YOUR RISK

Look at the strength and effectiveness of your organization's information security program:

- Nature of the program and how it has been implemented
  - Technical safeguards (e.g., encryption, security assessments/audits, firewalls, access control requirements)

  - Administrative safeguards (e.g., employee hiring and training practices)
  - Physical safeguards (e.g., access cards, access logs)
- Where data is stored (locally or in the cloud/on a third-party platform)
- With whom data is shared

Develop hypothetical breach scenarios based on your organization’s posture:

- If you rely on **credit card payments**, you may incur fees from credit card companies or payment processors if you suffer a data breach
- If you collect and store **personal information**, you may be concerned about user notification and related expenses
- If you store large amounts of valuable but non-personal information, you may worry about data restoration costs
- You may be particularly susceptible to **insider threats** or **rogue employees**
- You may be concerned about **hackers** and other outside threats, including phishing and other forms of **social engineering** (i.e., attempts to impersonate another employee or a trusted third party)

CYBER COVERAGE FOR LOSSES

Cyber insurance will typically cover the following types of first-party losses:

- Legal costs to determine your notification obligations and other regulatory requirements
- Recovery and replacement of lost or stolen data
- Customer notification and call center services
- Providing credit monitoring and other mitigation services
- Lost income due to business interruption
- Additional security training for employees and consultants
- Creating security policies and templates
- Crisis management and public relations costs
- Cyber extortion and fraud
- Theft of intellectual property or sensitive data
- Denial of service attacks
- Forensic services to investigate the breach
- Fees, fines and penalties related to the security incident

Cyber insurance will typically cover the following types of third-party losses:

- Payments to individuals affected by the breach
- Claims and settlement expenses relating to disputes or lawsuits
- Losses related to defamation and copyright or trademark infringement
- Costs for litigation and responding to regulatory inquiries
- Other settlements, damages and judgments
- Accounting costs

THE APPLICATION PROCESS

In assessing your eligibility for cyber coverage, an insurer will typically request the following information:

- Composition of information security team/function (if any)
- Percentage of total IT budget allocated to security
- Technical, administrative and physical safeguards your organization currently employs
- Any third party controls (e.g., audits of third-party service providers, vendor contracts)
- Data backups
- Policies
    - Internal and external privacy and data use policies
    - Network security and training policies
    - Network access/acceptable use policies (e.g., social media policies, email policies, "bring your own device" (BYOD) policies
    - Records and information management policies
    - Data destruction policies
    - Incident response plans

COVERAGE CONDITIONS

Before issuing your policy, the insurer may require your organization to:

- Implement encryption
- Undertake a security audit
- Deploy specific technical, administrative or other security enhancements

Even if the insurer doesn't require these measures, it may offer you a premium discount if you implement them.

You should weigh costs vs. benefits: can you really afford to implement any conditions of coverage (or engage a third-party provider that already has the measures in place)?

SUMMARY

Unfortunately, cyber insurance can be very expensive, and your organization may find that it cannot afford coverage. If that is the case, it is even more important to take other steps to protect your organization and mitigate potential risks of a security incident (see p. 1 of this article). In addition, even if your organization does not itself have cyber insurance, it is important to determine whether any third party provider(s) that host your organization's data have such coverage, as well as whether they implement the other safeguards noted above.

FURTHER INFORMATION

Here are some links to further information and additional resources:
National Council of Nonprofits, Cybersecurity for Nonprofits
Nonprofit Risk Management Center, *Data Privacy and Cyber Liability: What You Don't Know Puts Your Mission at Risk*
PBPA Webcast: Avoiding Fraud and Cyber Risk from Inside and Outside Your Nonprofit