Emerald Coast
MEDICAL ASSOCIATION

Announcing the ECMA Cyber Insurance Program

Buying that cyber policy you keep putting off just might be one of the best decisions you will ever make.

Rather than paying the ransom and having to deal with all of the headaches, problems, HIPAA violations triggered by the attack, and costs associated with a breach, a solid cyber insurance policy will give you much more than just peace of mind. One call can get a team of experts at your defense, covering expenses and taking your practice back!

And now, through the ECMA Cyber Insurance Program, we're making it easy for you to find the coverage that best fits your needs, because no two practices are alike.

- Our platform has access to seven AM Best "A" rated carriers
- Quick turnaround - answer just five questions and you will have up to five quotes in 24 hours or less*
- Quote Comparison breaking out key coverage limits in quoting carriers
- Full Prior Acts (overs claims arising from acts that took place at any time prior to the inception date of the policy)
- Up to $5M limits available with 2 of the markets (Otherwise up to $3M limit)

**Must be claims free*

Today, virtually every organization relies on data, so no one is immune from cyber threats. We appreciate the opportunity to partner with you to protect your digital assets with the right insurance coverages.

This ECMA Program is now being offered to you and your members.

For any questions, please contact:

Julie Danna
Senior Vice President | National Health Care Practice
(850) 530-3924
jdanna@risk-strategies.com

Michelle Flaat
Executive Director | Emerald Coast Medical Association
(850) 784-2090
michelle@flmedical.org

RISK strategies

ONE80 INTERMEDIARIES

CFMSE
Conference of Florida Medical Society Executives

Emerald Coast
MEDICAL ASSOCIATION

ECMA Cyber Insurance Program FAQ

WHAT IS CYBER INSURANCE?
When a breach occurs, cyber insurance covers the range of expenses that arise. These include identifying and solving the breach, recovering data, customer notifications, PR costs, possible credit monitoring expenses, legal expenses, potential fines from compliance regulators, extortion costs from ransomware, and general business interruption.

DO HACKERS REALLY BOTHER WITH ATTACKING SMALL BUSINESSES?
Yes. Hackers use technology to scan the internet for businesses with weak defenses regardless of the size of the business. A recent Verizon report notes that 43% of all cyber attacks are against small businesses. Worse, 63% of small businesses had experienced a breach in the last 12 months. Any business with a computer and an internet connection is at risk - even if you don't sell anything on yourwebsite.

WHAT'S COVERED?
First-party coverage - Covers damages a business suffers because of a cyber breach. This can include things like investigative services, business interruption coverage and data recovery.

Third-party coverage - Covers damages if a business' customers or partners are affected by a cyber attack. This can include legal fees, settlement costs, security failures and media liabilities.

Cyber crime - Covers damage due to any type of illegal activity that occurs using digital means. Examples of cybercrime are extortion/ ransomware, phishing, social engineering, and wire transfer fraud.

DOESN'T MY CURRENT BUSINESS INSURANCE INCLUDE CYBER ATTACKS?
Many general business policies only partially cover damage from cyber events, if at all. As mentioned above cyber coverage protects against the vast array of possible damages, expenses, and lost business that can occur from a cyber attack.

WHAT SHOULD I CONSIDER WHEN CHOOSING BETWEEN PURCHASING A STAND-ALONE CYBER POLICY VS. ADDING AN ENDORSEMENT TO AN EXISTING POLICY?
To be fully protected, ensure you have all coverages – first-party, third-party, and cyber crime. Further, since some cyber events can result in large expenses, confirm you have adequate sublimits for each of three above coverages.

WHY DO I NEED A "BREACH COACH"?
If your company gets hacked, you will need a breach coach to get your business back up and running fast. When a breach occurs, you need to assess and contain the damage, notify affected parties (e.g. customers and vendors), evaluate and act on the legal ramifications from agitated customers to regulatory bodies, and more. A breach coach will quickly assemble the right response team to deal with these issues. Without an expert it all falls on you, costing you time and money while adversely affecting your business. Fortunately, most insurance companies now provide a breach coach as part of a greater suite of services when you purchase stand-alone cyber insurance coverage.

DO SMALL BUSINESSES NEED CYBER INSURANCE IF THEY PRACTICE GOOD CYBER HYGIENE?
Being properly protected definitely helps. However, there is no way to fully protect against new threats or human error. Hackers are always adapting to overcome cyber defenses with new versions of current threats or creating brand new methods of attacking businesses. However damaging a new threat can be, the single biggest contributor to a breach is human error. Easy-to-hack passwords, phishing emails, or even a lost laptop all present potential entry points for a cyber criminal. Finally, a third-party vendor could be attacked impacting your ability to do business. A thorough cyber insurance policy is part of your overall risk management plan to ensure your business runs

* All of the above are general terms which may vary based on context. Please consult the policy form or ask an agent/broker for precise definitions and details.

For any questions, please contact:

Julie Danna
Senior Vice President | National Health Care Practice
(850) 530-3924
jdanna@risk-strategies.com

Michelle Flaat
Executive Director | Emerald Coast Medical Association
(850) 784-2090
michelle@flmedical.org

RISK strategies
ONE80 INTERMEDIARIES
CFMSE Conference of Florida Medical Society Executives

Emerald Coast MEDICAL ASSOCIATION

ONE80 INTERMEDIARIES

Claims Scenario

Ransomeware | Retail Trade

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

An employee of a music instrument retailer accidentally clicked on a malware link. The virus was downloaded onto the company server causing all data to be encrypted. The employee then received an email demanding $50,000 paid in Bitcoin within 48 hours to release their data files.

2,000 customer records including name, address, phone, and credit card information were encrypted. The retailer called their insurance company's cyber response team, who responded by assigning a "breach coach," which is covered as part of the retailer's stand-alone cyber policy.

The breach coach sent in a forensics team to assess the situation, including any computer or electronic hardware damage, and determine if paying the ransom was necessary. Concurrently, the insurance company confirmed coverage and assisted with opening a claim to minimize the effect of business interruption.

POTENTIAL IMPACT

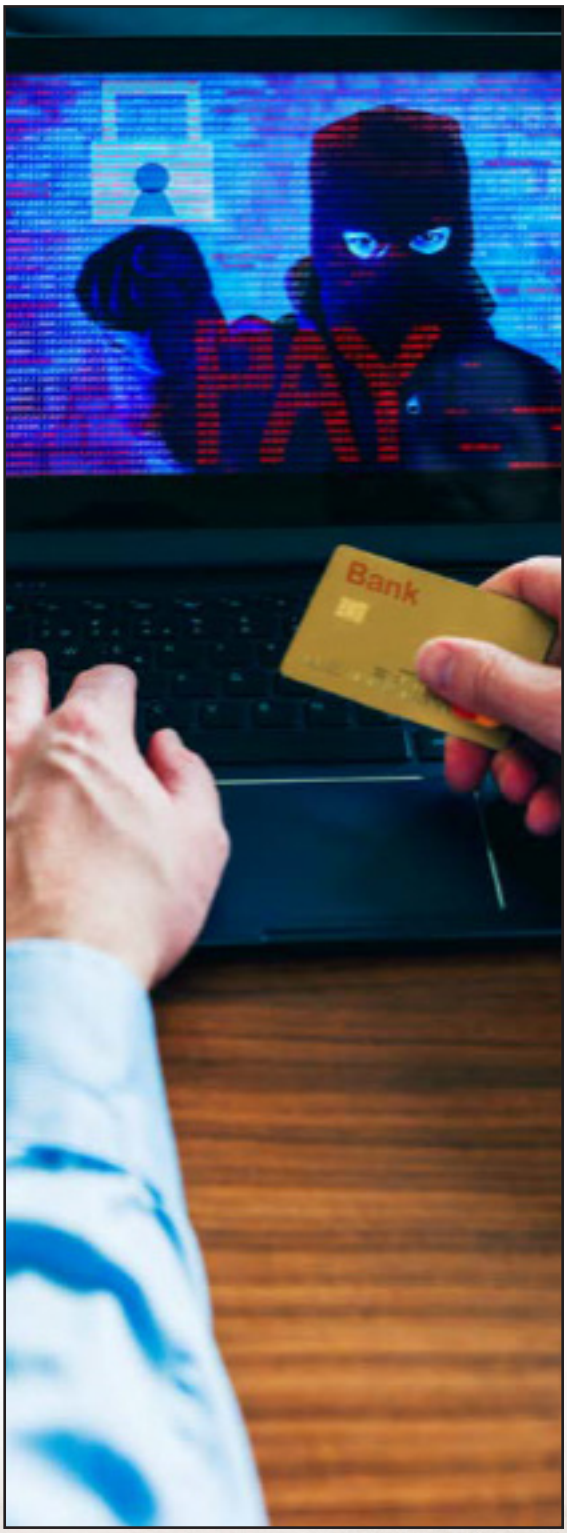
INCIDENT RESPONSE	
Incident response manager ("breach coach") fees	**$ 5,500**
Forensic investigation costs to locate malware, analyze damage, ensure containment and calculate loss	**$ 6,860**
Legal fees	**$ 4,000**
NOTIFICATION COSTS	**$ 1,230**
BUSINESS INTERRUPTION	**$ 31,325**
DATA RECOVERY Costs associated with replacing lost or corrupted data	**$ 10,100**
EXTORTION/RANSOMWARE Ransom payment	**$ 50,000**
BRICKING Damage to computer and hardware systems	**$ 12,050**
TOTAL	**$ 121,065**

RESOLUTION

While the business maintained regular back-ups online, the hackers also encrypted these files leaving the retailer no way to restore the data. The insurance company and breach coach agreed the fastest, best way to get the business back up and running was to pay the ransom.

The insurance company immediately paid the ransom via their pre-established Bitcoin account, releasing the records back to the retailer.

The swift assessment and payment, minimized the business interruption allowing the retailer to resume operations.



SAYATA LABS

Emerald Coast MEDICAL ASSOCIATION

ONE80 INTERMEDIARIES

Claims Scenario

SOCIAL ENGINEERING | Finance and Insurance

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A mortgage broker's emails were accessed by an attacker who, posing as the General Manager, asked an employee to contact the broker's bank with instructions for funds to be transferred into the hacker's bank account.

When the mortgage broker discovered that unauthorized payments were made totaling $425,000, they immediately contacted their bank to freeze the funds and notified their cyber insurance carrier. Together, they were able to recover $354,000 of the unauthorized transactions.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to locate the breach, analyze damage, and ensure containment	$ 13,500
Legal fees	$ 9,500
FUNDS TRANSFER FRAUD **Transferred funds not recovered**	$ 71,000
TOTAL	$ 94,000

RESOLUTION

The mortgage broker has a stand-alone cyber policy that covers social engineering as well as provides crucial response services. Once the broker notified their insurance company, an IT forensic consultant was appointed to assist the broker in repairing the damage to their system as well as to prevent future attacks.

As the mortgage broker has expanded cyber crime coverage under their policy, they were reimbursed for the direct financial loss, less the deductible, of the unrecovered fraudulent transfers as well as their forensic and legal costs.

SAYATA LABS

Emerald Coast MEDICAL ASSOCIATION

ONE80 INTERMEDIARIES

Claims Scenario

OUTDATED SOFTWARE | Educational Services

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

Hackers penetrated a graphic design school's network from a vulnerability in an outdated software application. 4,000 student names, addresses, emails, bank details and school records were compromised.

Local authorities received multiple complaints of suspicious activity, leading the school's IT department to discover an unauthorized user had accessed the system.

Once discovered, the school called their insurance carrier who immediately brought in forensic experts to initiate the school's IT recovery plan and notification program.

POTENTIAL IMPACT

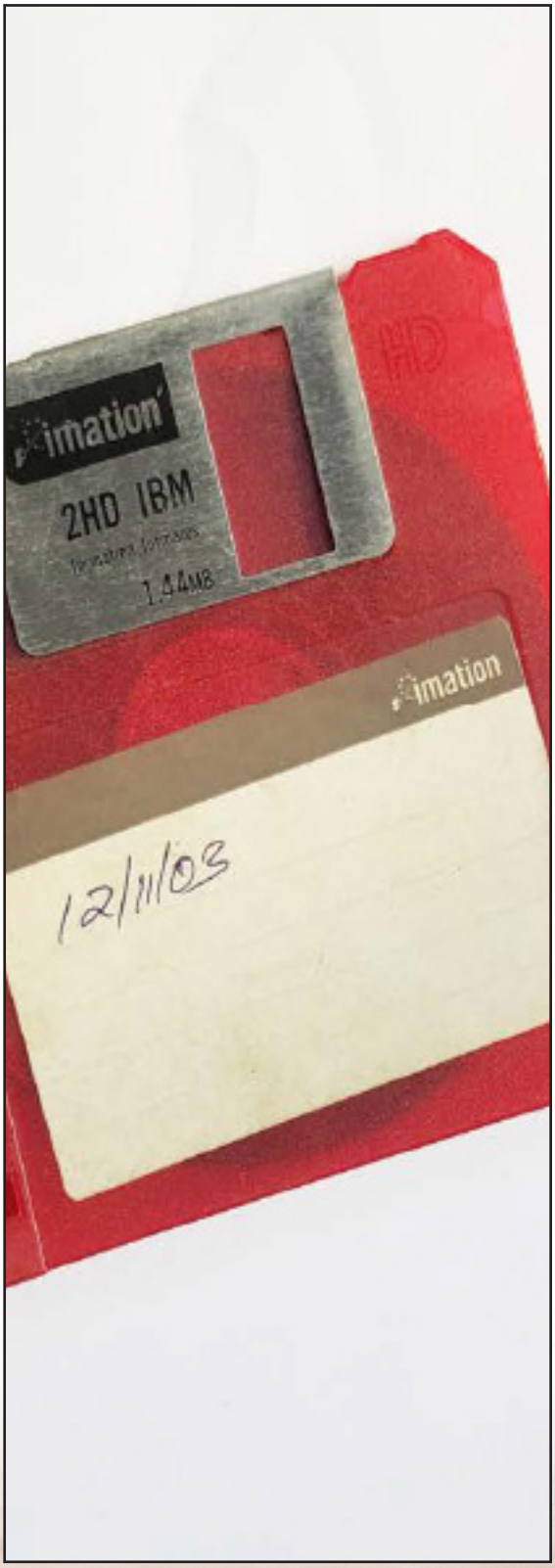
INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	**$ 11,850**
Identity theft and credit monitoring services	**$ 11,500**
Incident response fees	**$ 7,850**
Public relations fees to minimize reputational impact	**$ 10,050**
Call center set up and operation to field inquiries	**$ 10,200**
NOTIFICATION COSTS	**$ 1,865**
EXTORTION/RANSOMWARE DATA RECOVERY Costs associated with replacing lost or corrupted data	**$ 14,850**
REGULATORY	
Legal expenses arising from regulatory investigation due to mismanagement of private information	**$22,175**
Legal expenses and settlement costs for claims	**$16,100**
BUSINESS INTERRUPTION	**$39,318**
TOTAL	**$ 145,758**

RESOLUTION

The school's cyber policy was triggered, giving them immediate access to response services. The insurance company dispatched a forensic team who quickly isolated the unauthorized user.

A claim was started immediately to help with impending legal, consulting and media costs. The insurance company, IT team and forensic consultants ensured the school had up-to-date cyber defenses including firewalls, intrusion detection software, and encrypted databases. Concurrently, officials worked with local media to notify affected students and offer credit monitoring services, while the legal team handled the backlash from those affected.

Finally, the forensic consultants helped develop a new plan that included regular updates, testing, and education of all staff to minimize future breaches.



SAYATA LABS

Emerald Coast MEDICAL ASSOCIATION

ONE80 INTERMEDIARIES

Claims Scenario

LOST HARDWARE | Health Care and Social Assistance

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

An employee of a medical group lost their laptop. An Excel file on the computer contained medical records of 1,500 patients including the names, addresses, dates-of-birth, medical record numbers, medications, and diagnoses.

Once the loss was realized, the medical group immediately notified their insurance company who provided a "breach coach" to assess the damage and help the insured comply with regulatory and notification requirements.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic costs to assess and contain damage	$ 8,000
Legal Fees	$ 15,500
Public relations fees to minimize reputational impact	$ 10,000
NOTIFICATION COSTS	$ 1,250
DATA RECOVERY Costs associated with replacing lost or corrupted data	$ 9,550
REGULATORY Settlement fine	$ 25,000
Patient liability settlements	$ 52,250
TOTAL	$ 121,500

RESOLUTION

The breach coach assigned a forensics team, provided by the insurance company, to determine the potential exposure of the protected health information (PHI). It was determined that the patient PHI was, in fact, compromised. The patients were immediately notified and offered credit monitoring services.

Concurrently, the breach coach engaged a public relations agency to minimize the reputational damage as well as alerted counsel to help settle legal action from patients.

They were proactive in contacting the Department of Health and Human Service Office for Civil Rights and agreed upon a settlement amount as well as a corrective action plan that included employee cyber and data protection training.

SAYATA LABS

Emerald Coast MEDICAL ASSOCIATION

ONE80 INTERMEDIARIES

Claims Scenario

FORMER OR ROGUE EMPLOYEE | Arts, Entertainment, and Recreation

The following example is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A museum was hacked by a former employee, whose user credentials were not deleted when they were terminated. The employee sold 1,115 donor records on the dark web including name, address, email, and credit card number including expiry dates.

The museum notified their insurance company immediately. The carrier provided forensic expertise, legal services, and media relations help to investigate and control the damage.

In addition, the insurance company enlisted a "breach coach" to guide the museum in managing their actual and reputational damage.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to analyze damage and ensure containment	$ 7,600
Identity theft and credit monitoring services	$ 5,620
Legal fees	$ 9,935
Public relations fees to minimize reputational impact	$ 8,380
Call center set up and operation to field inquiries	$ 5,700
NOTIFICATION COSTS	$ 1,025
DATA RECOVERY Costs associated with replacing lost or corrupted data	$ 8,450
TOTAL	$ 46,710

RESOLUTION

The forensic team quickly identified the breach and worked with the museum's IT department to initiate repairs. The breach coach guided the museum to hire a call center to quickly inform affected donors, field questions, and offer identity protection and credit monitoring services to ensure trust going forward. The insurance company recommended seeking legal counsel to pursue civil action against the former employee.

Concurrently, the museum, in tandem with the media relations team, responded quickly and transparently to the media.

Finally, the insurance company and forensic team recommended an updated cyber response plan that included more rigorous IT policies and procedures as well as several technological updates to improve cyber hygiene. Due to the fast response, the costs and reputational damage to the museum were minimized.

SAYATA LABS