Cyber Attacks: A Threat to Public Entities

Presented by:

Susan M. Garvey, Director of Legal Services

Margie Zarcone, Supervisor of Liability Claim Operations

Intergovernmental Risk Management Agency

Member Panelists

Denyse Carreras, Village of Park Forest
Craig Kaufman, Village of Park Forest

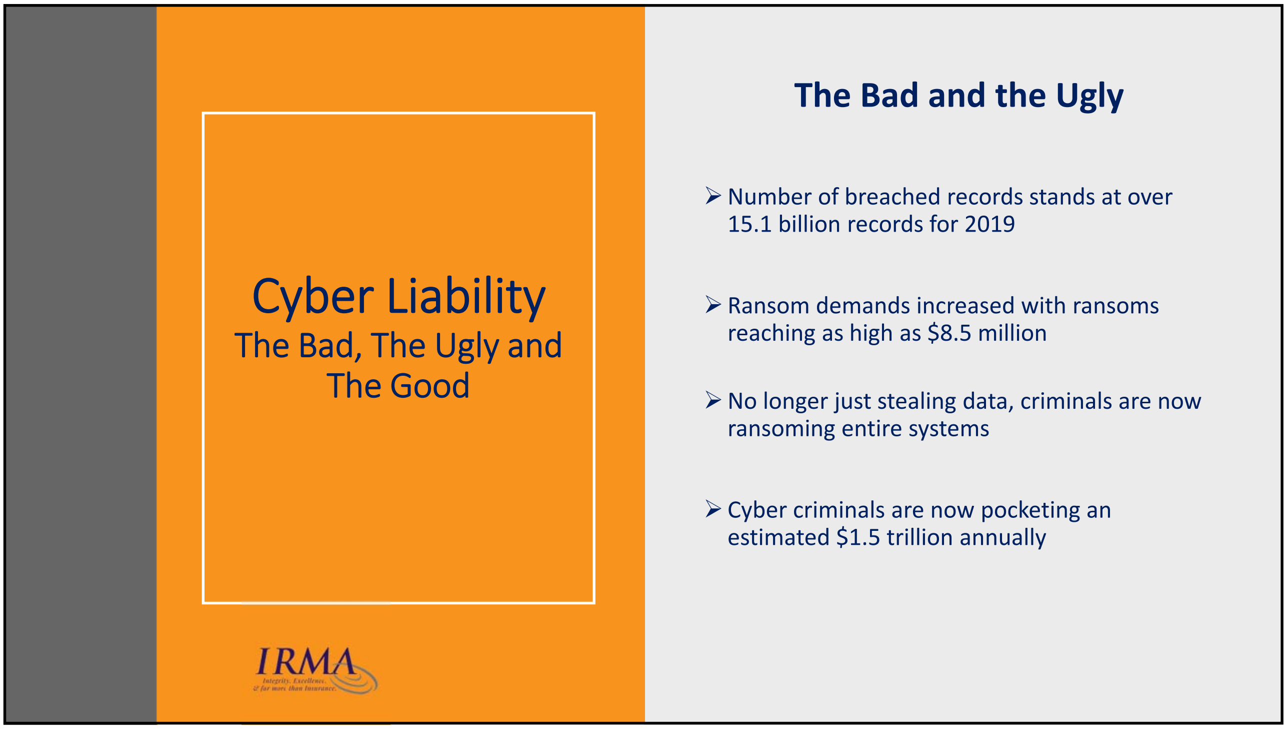
Michael Mertens, Village of Willowbrook

1

Agenda

- The Bad, The Ugly and the Good
- A Member's Story – Park Forest
- Cyber Exposures
- A Member's Story – Willowbrook
- IRMA's Cyber Coverage
- Making a Claim

2



Cyber Liability

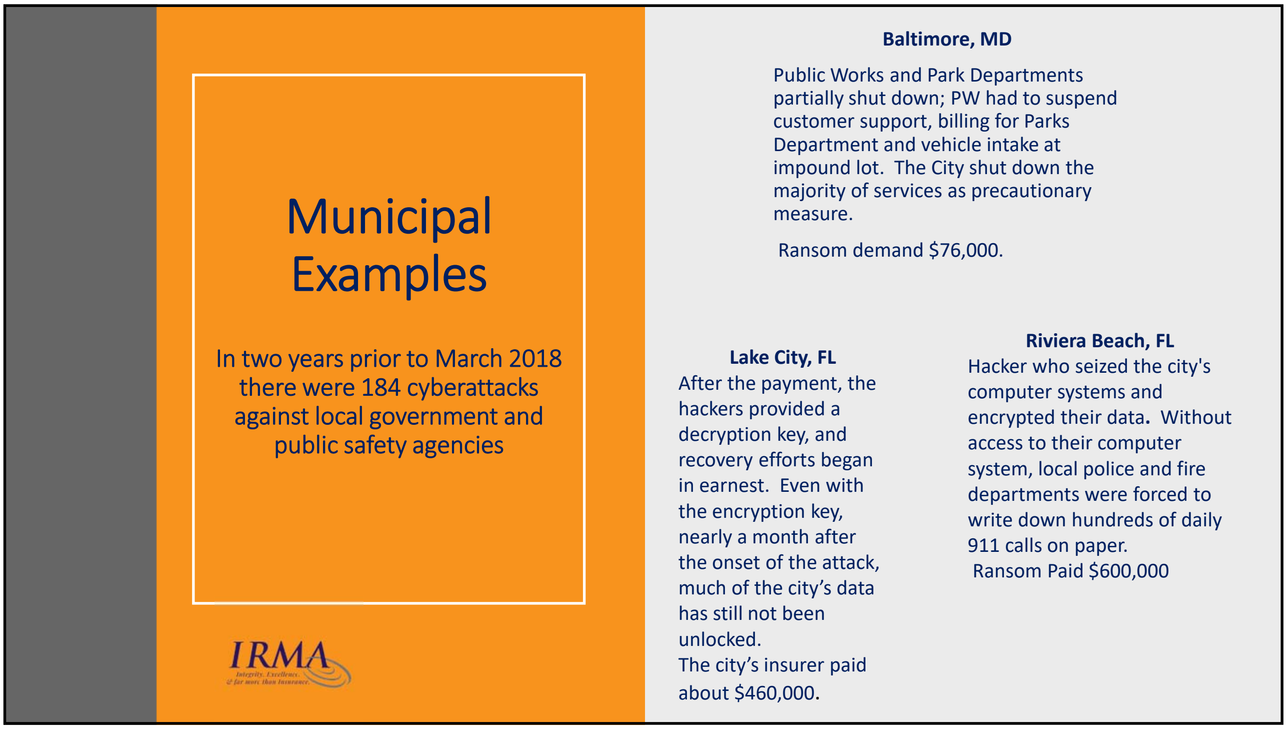
The Bad, The Ugly and The Good

IRMA

The Bad and the Ugly

- Number of breached records stands at over 15.1 billion records for 2019
- Ransom demands increased with ransoms reaching as high as $8.5 million
- No longer just stealing data, criminals are now ransoming entire systems
- Cyber criminals are now pocketing an estimated $1.5 trillion annually

3



Municipal Examples

In two years prior to March 2018 there were 184 cyberattacks against local government and public safety agencies

IRMA

Baltimore, MD

Public Works and Park Departments partially shut down; PW had to suspend customer support, billing for Parks Department and vehicle intake at impound lot. The City shut down the majority of services as precautionary measure.

Ransom demand $76,000.

Lake City, FL

After the payment, the hackers provided a decryption key, and recovery efforts began in earnest. Even with the encryption key, nearly a month after the onset of the attack, much of the city's data has still not been unlocked.

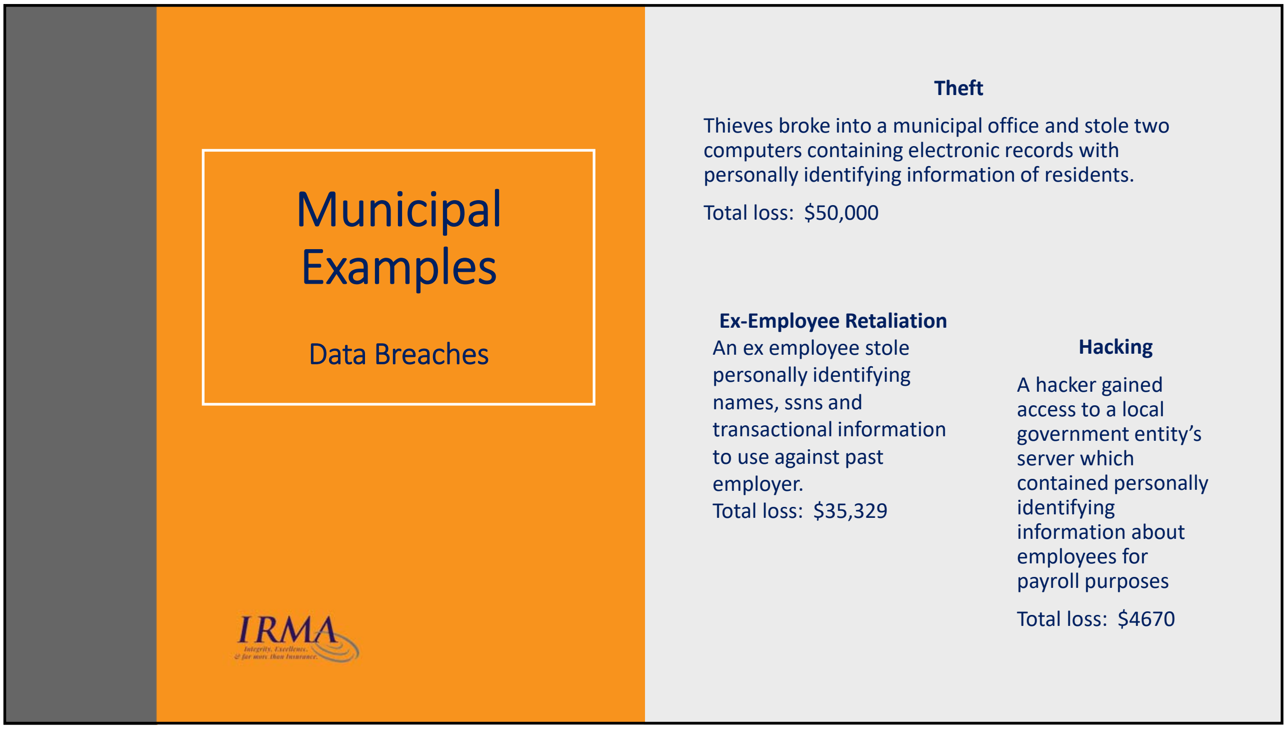
The city's insurer paid about $460,000.

Riviera Beach, FL

Hacker who seized the city's computer systems and encrypted their data**.** Without access to their computer system, local police and fire departments were forced to write down hundreds of daily 911 calls on paper.

Ransom Paid $600,000

4



Municipal Examples

Data Breaches

Theft

Thieves broke into a municipal office and stole two computers containing electronic records with personally identifying information of residents.

Total loss: $50,000

Ex-Employee Retaliation

An ex employee stole personally identifying names, ssns and transactional information to use against past employer.

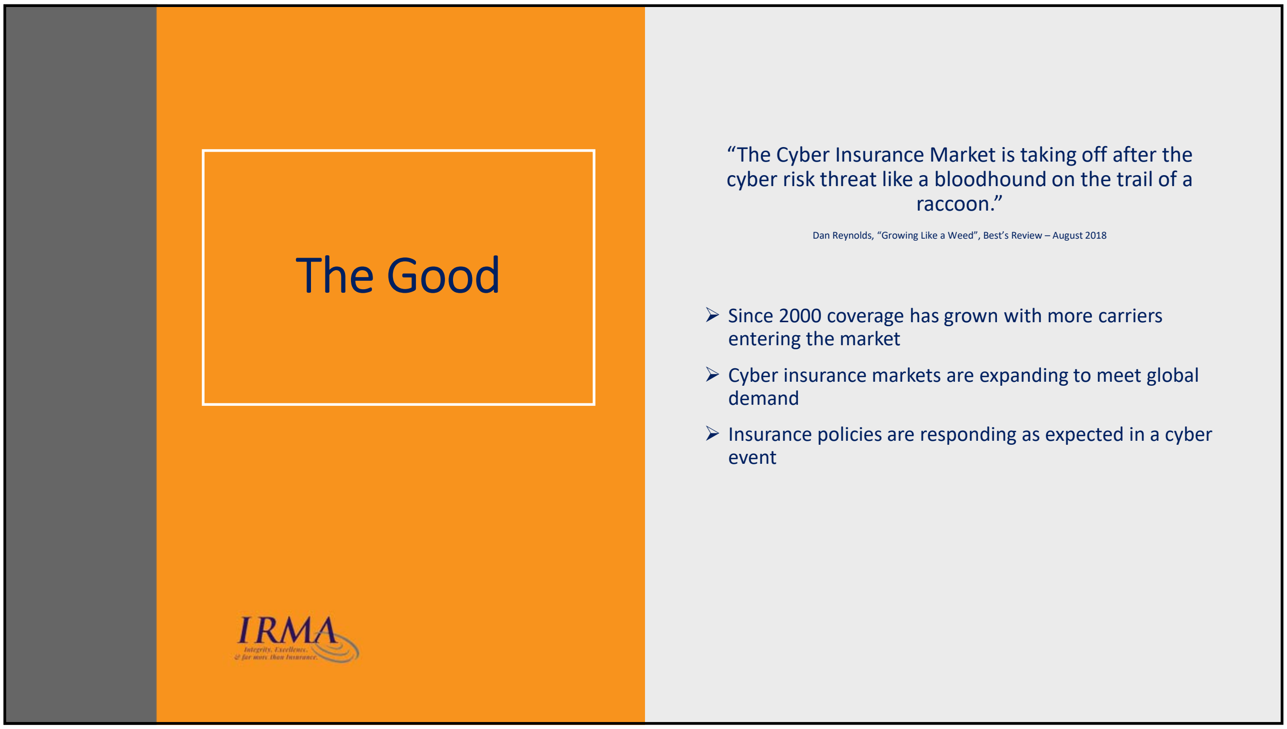
Total loss: $35,329

Hacking

A hacker gained access to a local government entity’s server which contained personally identifying information about employees for payroll purposes

Total loss: $4670

5



The Good

“The Cyber Insurance Market is taking off after the cyber risk threat like a bloodhound on the trail of a raccoon.”

Dan Reynolds, “Growing Like a Weed”, Best’s Review – August 2018

- ➢ Since 2000 coverage has grown with more carriers entering the market
- ➢ Cyber insurance markets are expanding to meet global demand
- ➢ Insurance policies are responding as expected in a cyber event

6

A Member's Story

Park Forest
Live Grow Discover

Ransomware Attack

August 28, 2019

Panelists:

Denyse Carreras, Director of Human Resources

Craig Kaufman, IT Administrator

IRMA
Integrity. Excellence.
& far more than Insurance.

7

The Team – Key Roles

The entire incident was handled by a key team with specific roles

Craig Kaufman – IT Administrator

- Worked with cyber security firm
- Determine if proprietary or personal information breach
- Determine what can be restored and safe restore period
- Determine how access was made and when

Denyse Carreras (Director of HR)

- Copied on all communications
- Worked closely with attorney, 3rd party cyber security firm and negotiators
- Getting employees paid
- Communication with Department Heads

IRMA
Integrity. Excellence.
& far more than Insurance.

8

The Team – Key Roles

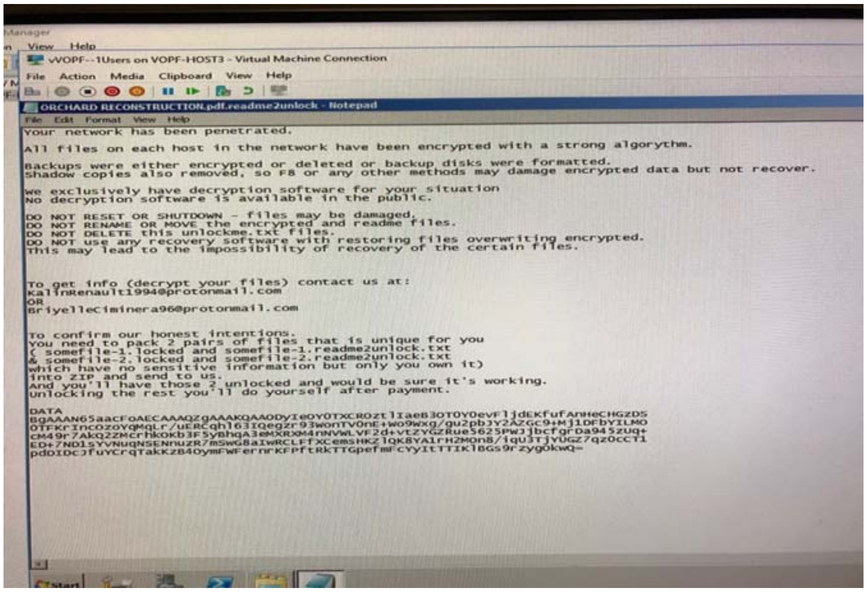
Tom Mick - Village Manager

- Keep Board apprised
- Determination of Village's financial ability
- Department head/employee communication

Mark Pries - Finance Director

- determine Village's financial ability. What was the max we would go
- Transfer of funds
- Manage payroll if we couldn't handle electronically
- Developing RFP/RFQs for new IT support contracts

9


Manager
View Help
vWOPF--1Users on VOPF-HOST3 - Virtual Machine Connection
File Action Media Clipboard View Help
ORCHARD RECONSTRUCTION.pdf.readme2unlock - Notepad
File Edit Format View Help

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE this unlockme.txt files.
DO NOT use any recovery software with restoring files overwriting encrypted.
This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at:
KalinRenault1994@protonmail.com
OR
BriyelleCiminera96@protonmail.com


To confirm our honest intentions.
You need to pack 2 pairs of files that is unique for you
( somefile-1.locked and somefile-1.readme2unlock.txt
& somefile-2.locked and somefile-2.readme2unlock.txt
which have no sensitive information but only you own it)
into ZIP and send to us.
And you'll have those 2 unlocked and would be sure it's working.
Unlocking the rest you'll do yourself after payment.

DATA
```

BgAAAN65aacFoAECAAAQZgAAAKQAAODyIeOY0TXCROztlIaeB3OTOYOevFljdEKfufAnHeCHGzD5
0TFKrIncOzoYqMqLr/uERCqhl63IQegzr93wonTV0nE+Wo9Wxg/gu2pbJY2AZGc9+Mj1DFbYILMO
cM49r7AkQ2ZMcrhkOKb3F5yBhqA3eMXRXM4nNVWLVF2d+vtZYGZRue5625PWJjbcfgrDa945zUq+
ED+7ND1sYVNuqNSENnuzR7mSwG8aIWRCLFfXCemsHKZlQK8YA1rH2MOn8/iqU3TjYUGZ7qzOcCT1
pdOIDcJfuYCrqTakKzB4OymFWFernrKFPftRkTTGpefmFcYyItTTIKlBGs9rzygOkwQ=

10

Law Enforcement

- With PD called FBI Homeland Security to try to determine point of entry
- They took 1 laptop to offices for forensics.
- Their focus was not on recovery of data.
- They don't have the expertise and wasn't able to determine what 'group of bad actors' were the culprits.

11

Response to Attack

- Strategy on staff/internal communication
- Notified Margo and Susan
- Contact with Hartford Steam Boiler (HSB) our 3rd party cyber crime vendor
  - Enlisted contract with technical defense attorney, a cyber security firm and a negotiator with a bit-coin wallet
  - Reviewed contracts for above experts
  - Reached out to SpearTip – recommended Cyber security firm in St. Louis, MO
- We learned that bugs can be in our system and troll, gathering information. Could be over a period of weeks. Once the troll has determined it has captured enough information that might be of monitory value, the system shuts down. Additionally information may be sold to the highest bidder out on the dark web.

12

Response to Attack
Friday, August 30, 2019

- First team conference call with attorney, IRMA, HSB.
  - Set priorities for all team members
  - Needed to enlist other specialists:
    - Negotiator with bit wallet - Coveware
    - Cyber security firm to provide incident response and forensic study - SpearTip
- Obtained, reviewed and signed contracts.
- Important to use a technical defense attorney to maintain privilege of all internal communication.

13

Response to Attack
Friday, August 30, 2019

- Working around the clock to install new virtual servers on an existing physical server
- Determine what was encrypted vs. what was still usable
- Move good data to fresh virtual servers
- Recover data from backups and restore on the new virtual servers

14

Response to Attack
Saturday, August 31, 2019

- Two technicians from Speartip and I went around Village Hall, Police, and Fire to install new antivirus software as well as look for infections on existing computers
- Multiple computers were found to be infected
- The infected computers were running Symantec Endpoint Protection which did not find nor prevent the infections
- Speartip collected log files, screen shots, and other documentation of the infected computers
- Speartip also collected logs from routers to try and determine if any data was exported from our servers to an outside entity. No evidence of that was found
- By this time I had determined we had one system at the Police Department that was compromised with no backups available. This one document management system was for scanned evidence and was the single reason the Village decided to try to negotiate for the ransomware encryption key

Response to Attack
Monday-Tuesday, September 2 and 3, 2019

- Conference call with attorney and negotiator
  - How negotiations work
  - Best guess on demand
  - Anticipated length of time to reach a settlement.
  - Education on how Bad Actors (aka Threat Actors) go about their business.
- Coveware given settlement authority of $50,000
- Negotiations begin via email from Coveware to Bad Actors
- Initial demand for decryption key sent quickly:
  - $80,000 – “experts” told us this was unheard of to hear back to quickly. That should have been my first clue.
- Negotiated settlement by following day
  - $31,722.70 – no typo
- VOPF elated! Great! Far less than $50,000

Response to Attack
Wednesday, September 4, 2019

- Transferred funds per demand
- Where’s the decryption key?
  - Silence
  - More silence
  - More silence
- Coveware reports: Bad Actors want $80,000
- VOPF – Not happy! OK: vent, get angry – now Breathe! Let it go! (Harder for some than others)

17

Response to Attack
Thursday- Friday, September 5 and 6, 2019

- Instructed negotiators no more money
- Bad Actor new offer - $50,000
- Instructed negotiators to have no further communication with them.
- Multiple messages from negotiators
  - Bad actors getting impatient
  - Pay or they will destroy the decryption key
  - Weekend is coming “they won’t be happy”
- Biding time for Craig to still uncover documents.
- If they MUST respond – “tell them to go pound sand”.

18

Response to Attack
IT Administrator

- The process of restoring servers back to fully operational for users took about 2 weeks
- Every day or two I would restore a certain software for a department, I.E. our financial software first, then our Police department software the next few days, etc.
- After the initial 2 weeks to get most software working, I still had a lot of cleanup to do such as moving all virtual servers to the new host, then completely formatted the infected host server to install a new operating system fresh, then move some of the virtual servers back for load balancing
- Work was ongoing for about 4 to 5 weeks

19

Response to Attack
Monday, September 23, 2020

- When we paid the ransom, we also paid Coveware per our contract. Part of the contract was $1,500 for decryption. Since we didn't receive that service, I requested our $1,500 back.
- Later that day, I receive notification that Coveware was sent the decryption key.
- We don't really need it – Craig got us up back and running.
- Finally agreed to have it sent to SpearTip and let them run it to reassure us it hasn't been encrypted with Malware. Came back fine.
- Instructions sent to Craig on how to deploy. Didn't give us anything we didn't already have thanks to Craig!

20

In the End

- No customer personal information was breached
- 4 weeks no emails
- No lost data
- Few more grey hairs
- A bit wiser

21

Take Aways

- Breathe!
- Call Margo and Susan!
- Breathe!
- Even though we engage with experts, they work for us – don't be afraid to ask questions. Cyber crime is tricky, and experts speak very specific technical language that many of us have never even heard of. Ask for clarification.
- Closely manage and document every step actions and all expenses.
- Enlist Cyber attorneys – all communication is privileged as long as they are copied – not subject to FOIA. Corporate attorneys won't cut it.
- The bad actors are watching – be cautious on what is communicated internally and externally
  Perhaps not jump on first negotiated ransom demand
- Limit communications on need to know basis –
  - Pros –
    - Ability to control information to avoid speculation and leaks (we were being watched – could result in higher demand)
      Things were changing hourly and too much to keep updating everyone on
      Maintaining privileged communication and potential exposure of those called to testify in any matter.
  - Cons-
    - Some people felt left out, not trusted
      Questions weren't being answered to their liking

22

Fixes Moving Forward

- More robust infrastructure
- Budgetary impact - We made the decision to restructure our IT department to be able to employ specialty services. This resulted in structuring a separation agreement with our IT Tech.
- Cyber security software
- Back-up solution
- 3rd party IT support solution
- Margo has negotiated an extremely more robust Cyber Security Coverage for the membership

23

Cyber Liability Exposure

- Data Compromise and Breach
- Data Compromise Liability
- Cyber Attack
- Ransomware and Extortion

24

Data Breach

What is a Breach?

The unauthorized exposure of personally identifiable information

Unauthorized Exposure

- Loss
- Physical Theft
- Accidental Publication

Affected Individuals

Employees, residents, 3rd parties

IRMA
Integrity. Excellence.
& far more than Insurance.

25

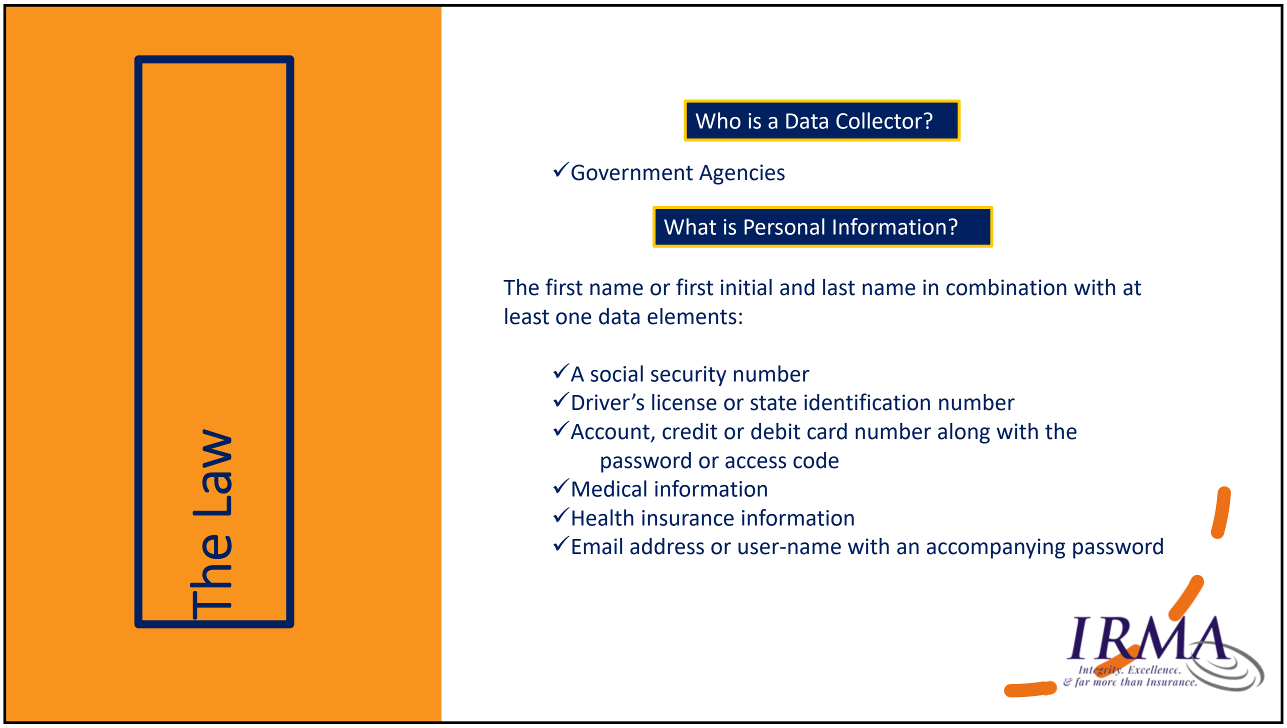
Data Breach – The Law

Personal Information Protection Act
815 ILCS 530/1 – 530/25
Effective January 1, 2017

Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach.

IRMA
Integrity. Excellence.
& far more than Insurance.

26



The Law

Who is a Data Collector?

- ✓Government Agencies

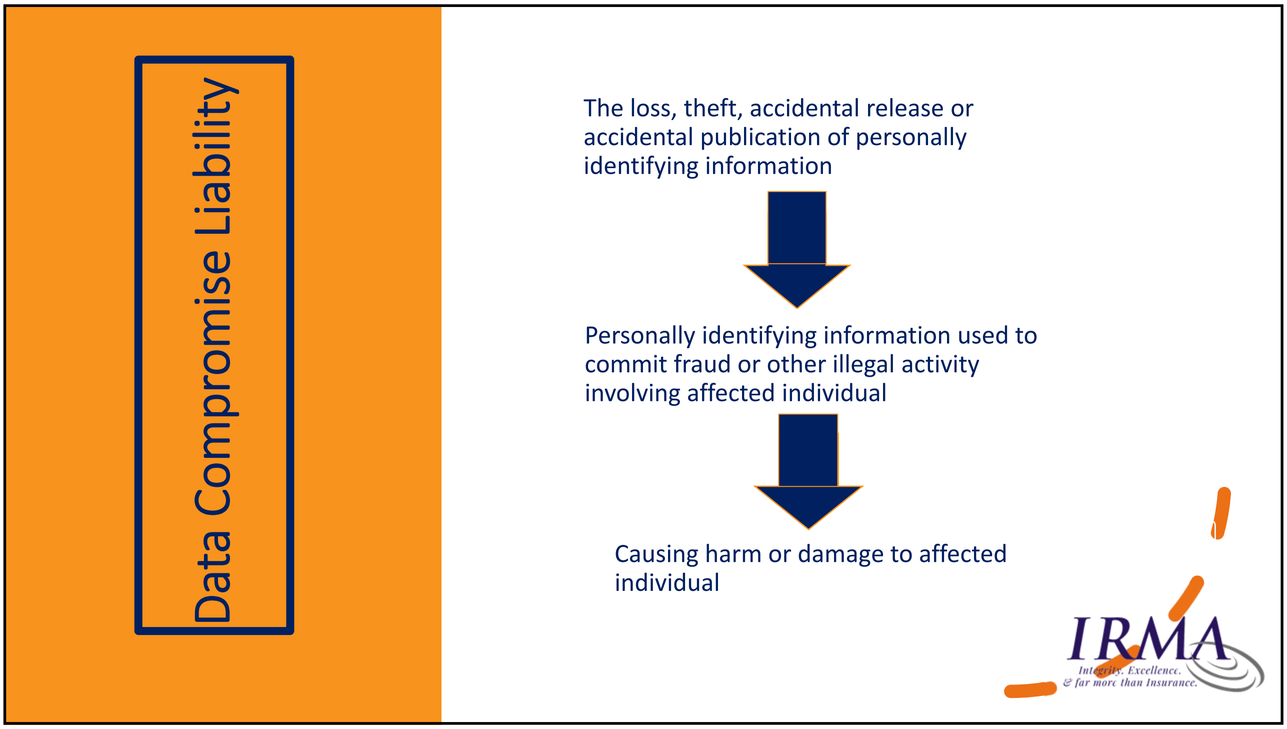
What is Personal Information?

The first name or first initial and last name in combination with at least one data elements:

- ✓A social security number
- ✓Driver's license or state identification number
- ✓Account, credit or debit card number along with the password or access code
- ✓Medical information
- ✓Health insurance information
- ✓Email address or user-name with an accompanying password

IRMA
Integrity. Excellence.
& far more than Insurance.

27



Data Compromise Liability

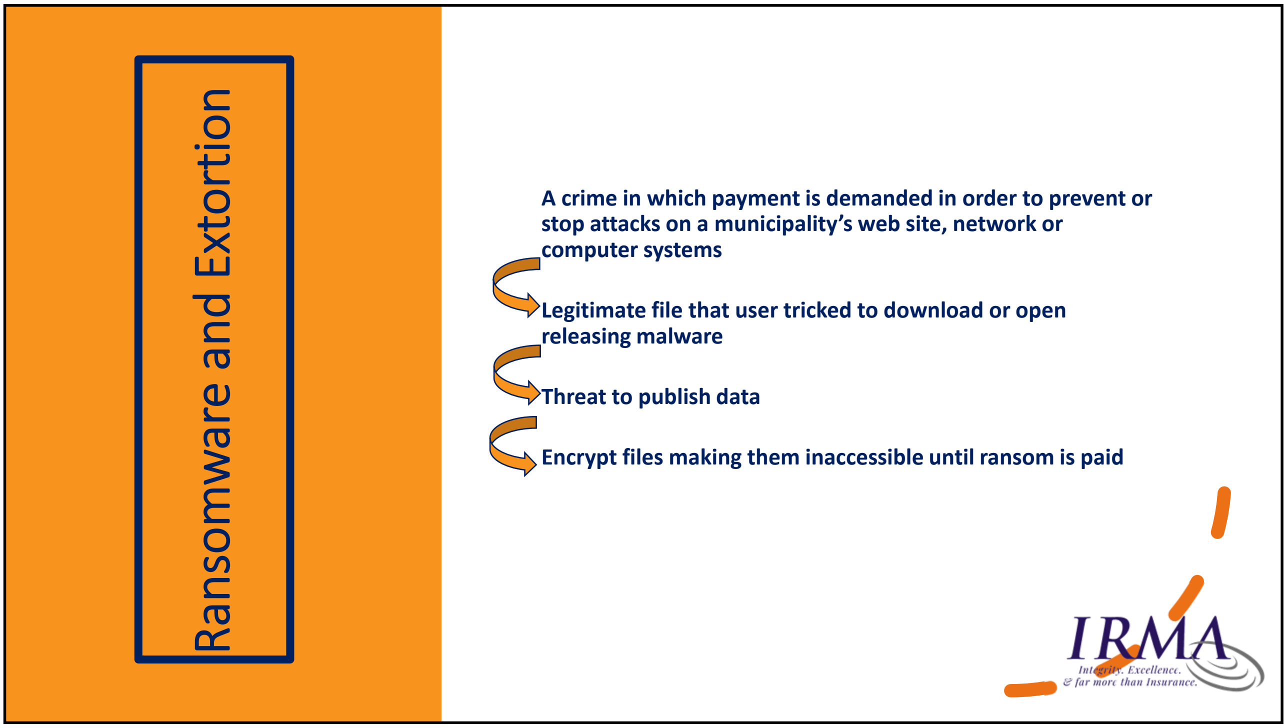
The loss, theft, accidental release or accidental publication of personally identifying information

Personally identifying information used to commit fraud or other illegal activity involving affected individual

Causing harm or damage to affected individual

IRMA
Integrity. Excellence.
& far more than Insurance.

28



Ransomware and Extortion

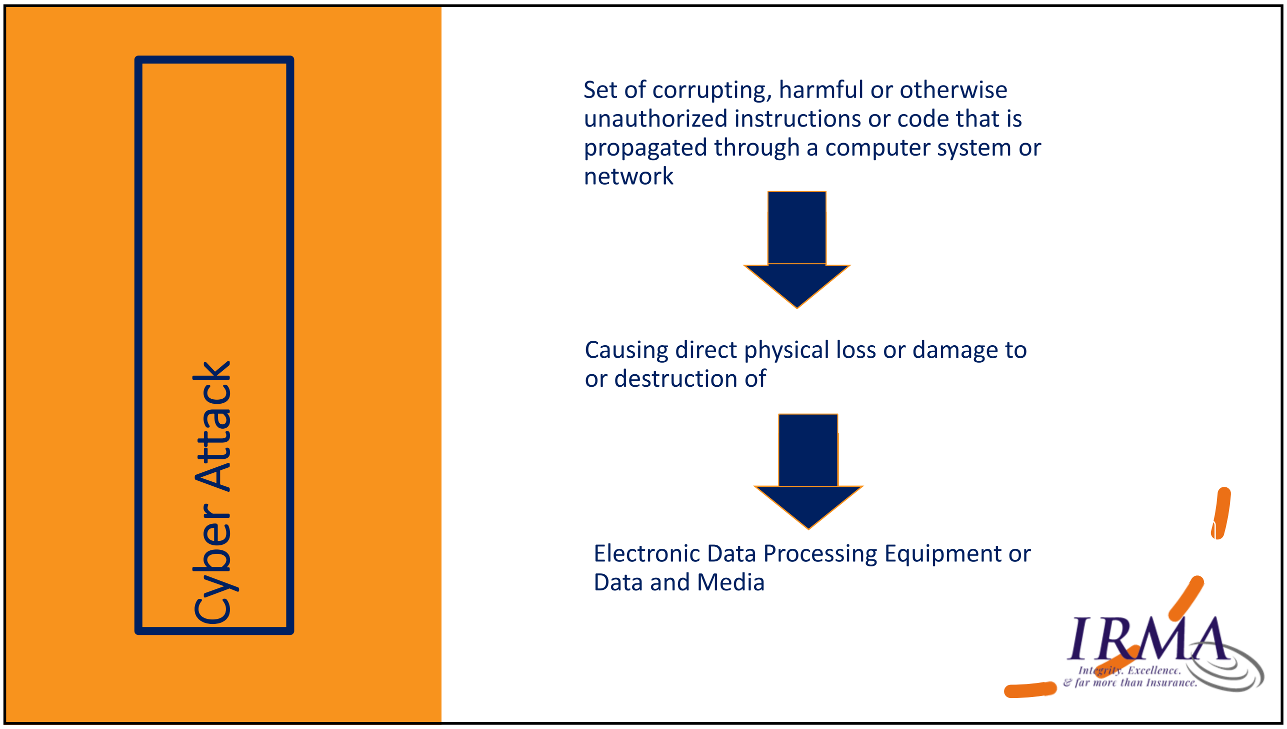
A crime in which payment is demanded in order to prevent or stop attacks on a municipality's web site, network or computer systems

- Legitimate file that user tricked to download or open releasing malware
- Threat to publish data
- Encrypt files making them inaccessible until ransom is paid

IRMA

Integrity. Excellence. & far more than Insurance.

29



Cyber Attack

Set of corrupting, harmful or otherwise unauthorized instructions or code that is propagated through a computer system or network

Causing direct physical loss or damage to or destruction of

Electronic Data Processing Equipment or Data and Media

IRMA

Integrity. Excellence. & far more than Insurance.

30

A Member's Story

IRMA
Integrity. Excellence.
& far more than Insurance.

VILLAGE OF WILLOWBROOK

Ransomware Attack

March 6, 2020

Panelist:

Michael Mertens, Assistant Village Administrator

31

Village of Willowbrook Cyber Attack

- The incident was first noticed Friday, March 6, 2020 at our Public Works Water Tower by our Public Works Foreman when he tried to log onto his machine.
- A notepad came onto his screen and advised:

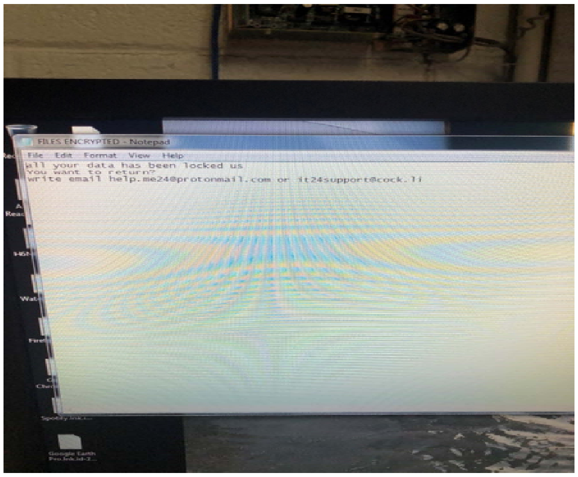
All your data has been locked us
You want to return?
write an email help.me24@prontomail.com or
it24support@cock.li

- Our Public Works Foreman advised our Finance Director via text about the incident.
- Our Finance Director at 6:36 am sent an email to all employees that our servers were down and contracted our IT representative who was on his way to our Village Hall.

IRMA
Integrity. Excellence.
& far more than Insurance.

32

Public Works Water Tower Computer



```
all your data has been locked us
You want to return?
write email help.me24@protonmail.com or it24support@cock.li
```

IRMA
Integrity. Excellence. & far more than Insurance.

33

Key Roles

- March 6, 2020 – 8 am. I walk in the door and our Public Works Foreman advised me that are servers were down and he thought we had been hacked. My first thought was this was a bad joke on a Friday morning.
- We triaged from my office with the Mayor, Administrator, Finance Director, and our IT Consultant reviewed the current status.
  - Servers were down.
  - Desktops were inaccessible.
  - Phone system was working.
  - Email was working.
  - Water system was operating.
- Our Finance Director manages our IT at the Village and she handled the communication with our IT consultant.
- Our Village Administrator managed communications with our Mayor and Board members, Police Department and neighboring agencies.
- I managed our IRMA and attorney contacts and centralized the incident information.

IRMA
Integrity. Excellence. & far more than Insurance.

34

Key Steps

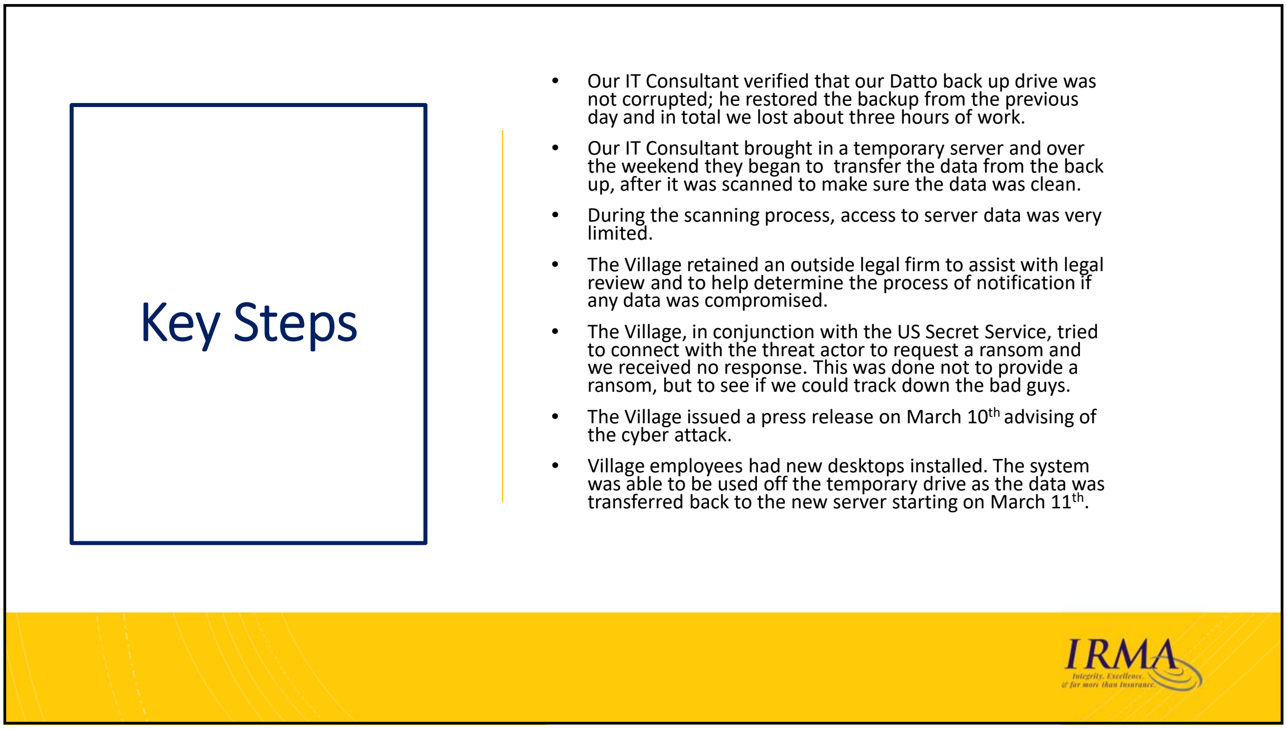
- We had our employees unplug their terminals and our IT contractor began working on the servers and backup drives.
  - Our file servers were corrupted.
  - Our file servers are backed up a Datto system that backs up to the cloud on a continuous basis and seemed intact.
  - Our e-mail server is backed up to the cloud so that system was not affected.
- We notified our Village Board members, Du-Comm, Tri-state Fire Protection District, DuPage Water Commission, etc.
- I called IRMA to advise them of the cyber-attack. I spoke with Margie Zarcone a number of times. Margie put me in contact with Hartford Steam Boiler (HSB) who provides the cyber coverage for IRMA.
- We received a copy of the IRMA coverage policy and was put in contact with a representative with HSB who supplied the Village with a cyber incident response information sheet which highlighted Forensic IT Providers, Legal Firms and Credit Monitoring Firms.

35

Key Steps

- The Village Police Department reached out to the US Secret Service. Agents arrived on site that afternoon.
  - The agents conducted interviews and identified infrastructure
  - Forensic acquisition began with memory dumps collected
  - Control computers identified
  - Infected computers Identified
  - Hard drives collected (control HD & infected HD)
  - Infected servers collected
  - Identified potential ransomware Identified
- Individual hard drives in the Village were corrupted and any data stored on the individual desktops were lost.
- New server hard drives were ordered as well as new desktops for the staff. Luckily, the desktops were due for replacement in May 2020.

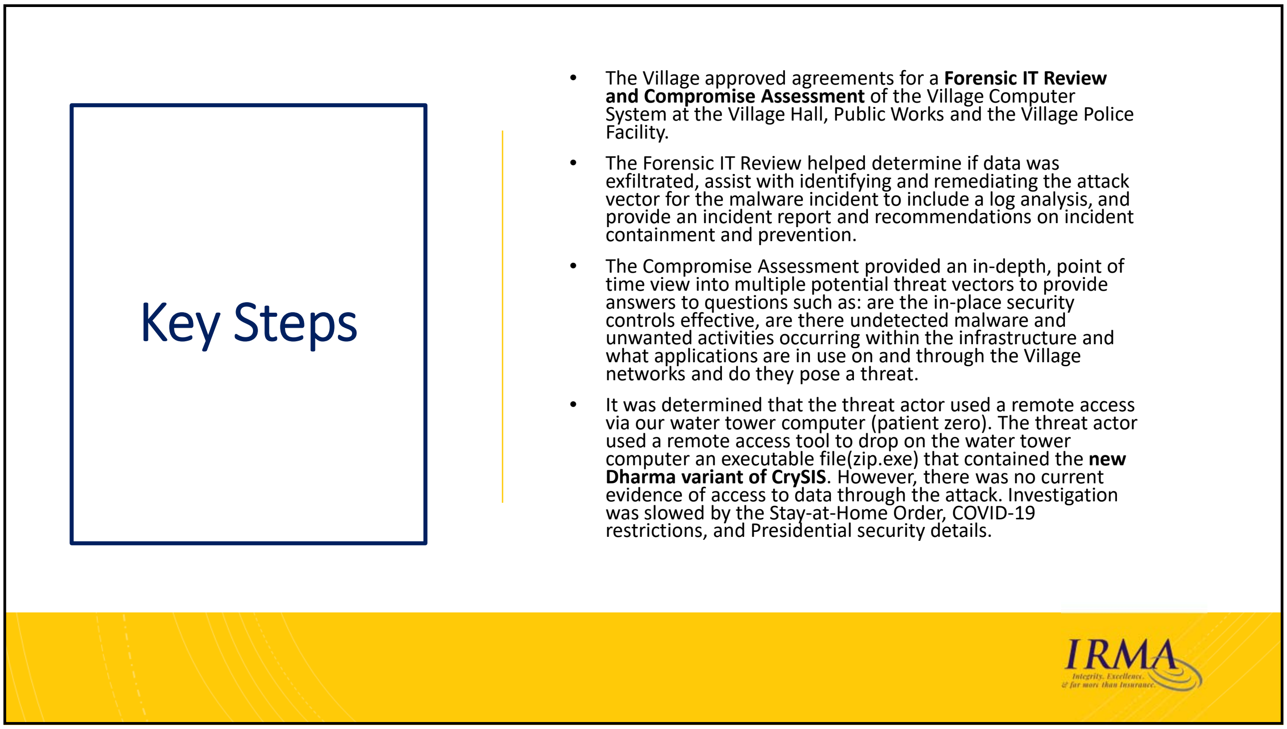
36



Key Steps

- Our IT Consultant verified that our Datto back up drive was not corrupted; he restored the backup from the previous day and in total we lost about three hours of work.
- Our IT Consultant brought in a temporary server and over the weekend they began to transfer the data from the back up, after it was scanned to make sure the data was clean.
- During the scanning process, access to server data was very limited.
- The Village retained an outside legal firm to assist with legal review and to help determine the process of notification if any data was compromised.
- The Village, in conjunction with the US Secret Service, tried to connect with the threat actor to request a ransom and we received no response. This was done not to provide a ransom, but to see if we could track down the bad guys.
- The Village issued a press release on March 10th advising of the cyber attack.
- Village employees had new desktops installed. The system was able to be used off the temporary drive as the data was transferred back to the new server starting on March 11th.

37



Key Steps

- The Village approved agreements for a **Forensic IT Review and Compromise Assessment** of the Village Computer System at the Village Hall, Public Works and the Village Police Facility.
- The Forensic IT Review helped determine if data was exfiltrated, assist with identifying and remediating the attack vector for the malware incident to include a log analysis, and provide an incident report and recommendations on incident containment and prevention.
- The Compromise Assessment provided an in-depth, point of time view into multiple potential threat vectors to provide answers to questions such as: are the in-place security controls effective, are there undetected malware and unwanted activities occurring within the infrastructure and what applications are in use on and through the Village networks and do they pose a threat.
- It was determined that the threat actor used a remote access via our water tower computer (patient zero). The threat actor used a remote access tool to drop on the water tower computer an executable file(zip.exe) that contained the **new Dharma variant of CrySIS**. However, there was no current evidence of access to data through the attack. Investigation was slowed by the Stay-at-Home Order, COVID-19 restrictions, and Presidential security details.

38

Claim Experience

- Hartford Steam Boiler (HSB) was involved in the pre-approval of key steps along the way. The communication was efficient between the claim representative, the Village legal team and IRMA.
- The IRMA Coverage is summarized as follows:
  - Data Compromise
  - Annual Aggregate Limit: $1,000,000
  - Sublimit of Forensic IT Review: $500,000
  - Sublimit of Legal Review: $500,000
  - Sublimit of Loss of Business: $500,000
  - Deductible: $10,000
- To date the Village spent $133,000 and was reimbursed $86,000. The difference was the $10,000 deductible and the new desktops we purchased in advance of our May 1 budget.

IRMA
Integrity. Excellence.
& far more than Insurance.

39

Take Aways

- Emergencies always seem to happen on Fridays.
- As with all emergencies the first couple of hours were chaotic.
- We outsource IT and they were great in responding but through the crisis we realized that we need a more universal approach to IT. Finance, Public Works, Community Development and Police all have their own needs and focus.
- We need an advocate to help sort through all of the IT advice that was provided.
- Train employees how to save their files properly and not just to their desktops.
- Software, hardware and IT are integral assets and need appropriate focus and budgets.

IRMA
Integrity. Excellence.
& far more than Insurance.

40

Going Forward

The Village is currently considering additional IT Analysis such as:

- **Security architecture reviews** are non-disruptive studies that uncover systemic security issues in your environment. This is a comprehensive assessment of the Village's entire environment, aimed at identifying in detail and prioritizing areas of improvement based on relative risk and impact.
- An **external penetration test** researches and attempts to exploit vulnerabilities that could be performed by an external user without proper access and permissions.
- An **internal penetration test** is similar to a vulnerability assessment; however, it takes a scan one step further by attempting to exploit the vulnerabilities and determine what information is actually exposed.
- **Social engineering penetration testing** comprises the techniques used by professional ethical hackers to trick a customer's staff into revealing sensitive information or perform the actions that create security holes for a hacker to slip through.

41

IRMA's Cyber Insurance

- Data Compromise Response Expenses Coverage
- Data Compromise Liability Insurance
- Cyber Extortion and Ransomware
- Computer Attack

42

Data Compromise Response Expense

Coverage Trigger

Unauthorized Exposure of Personally Identifiable Information

- Forensic Information Technology
  - Coverage to hire outside computer consultant
- Legal Review
  - Coverage to Consult with legal counsel
- Notification to Affected Individuals
  - Reimbursement of Expenses Associated with Notification
- Servicers to Affected Individuals
  - Information materials
  - Toll-free help-line
  - One-year credit monitoring
  - Identity Restoration Service
- Public Relations Services
- Costs for review of and response to potential impact

43

Data Compromise Liability

Coverage Trigger

Claim for Damages that Insured Legally Obligated to Pay

Must Arise out of covered loss under Response Expense coverage

- Civil proceeding in which damages to one or more affected individuals arising from personal data compromise are alleged

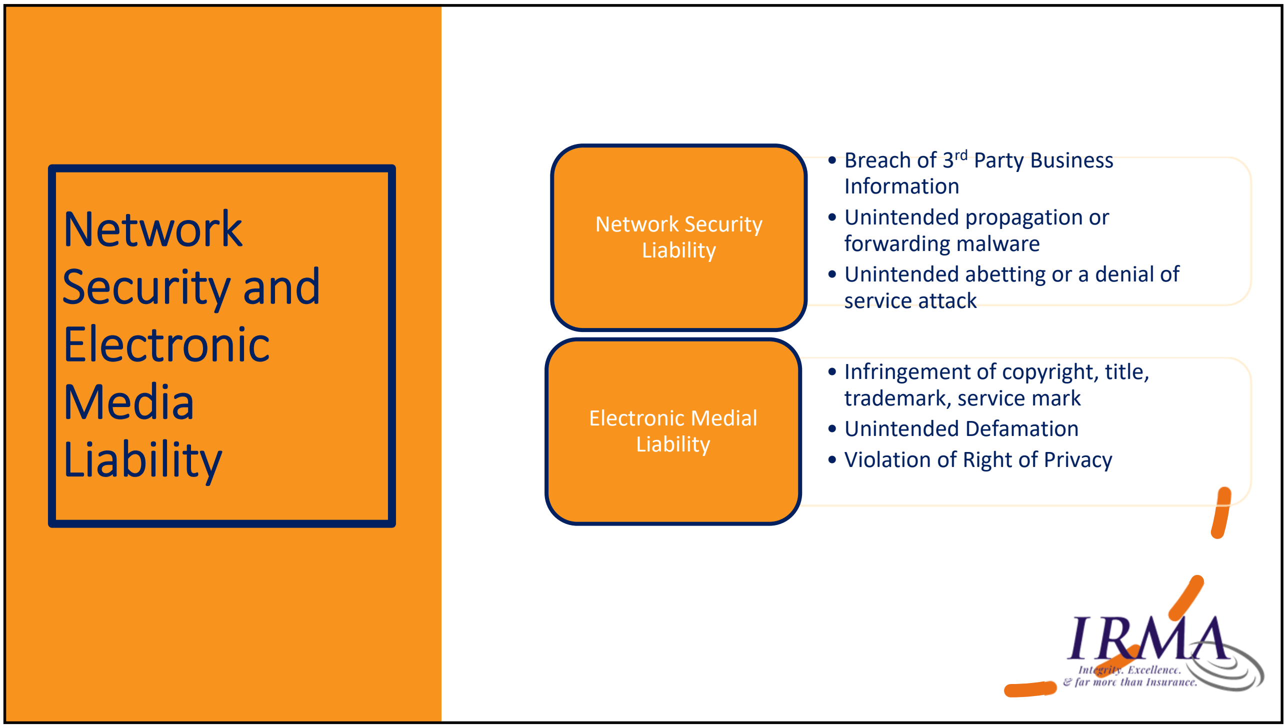
Data Compromise Liability

- Damages, judgments or settlements to affected individuals
- Defense Costs
- Prejudgment Interest

Defense Costs

- Expenses including attorney's fees resulting solely from the investigation, defense and appeal of any data compromise suit

44



Network Security and Electronic Media Liability

Network Security Liability

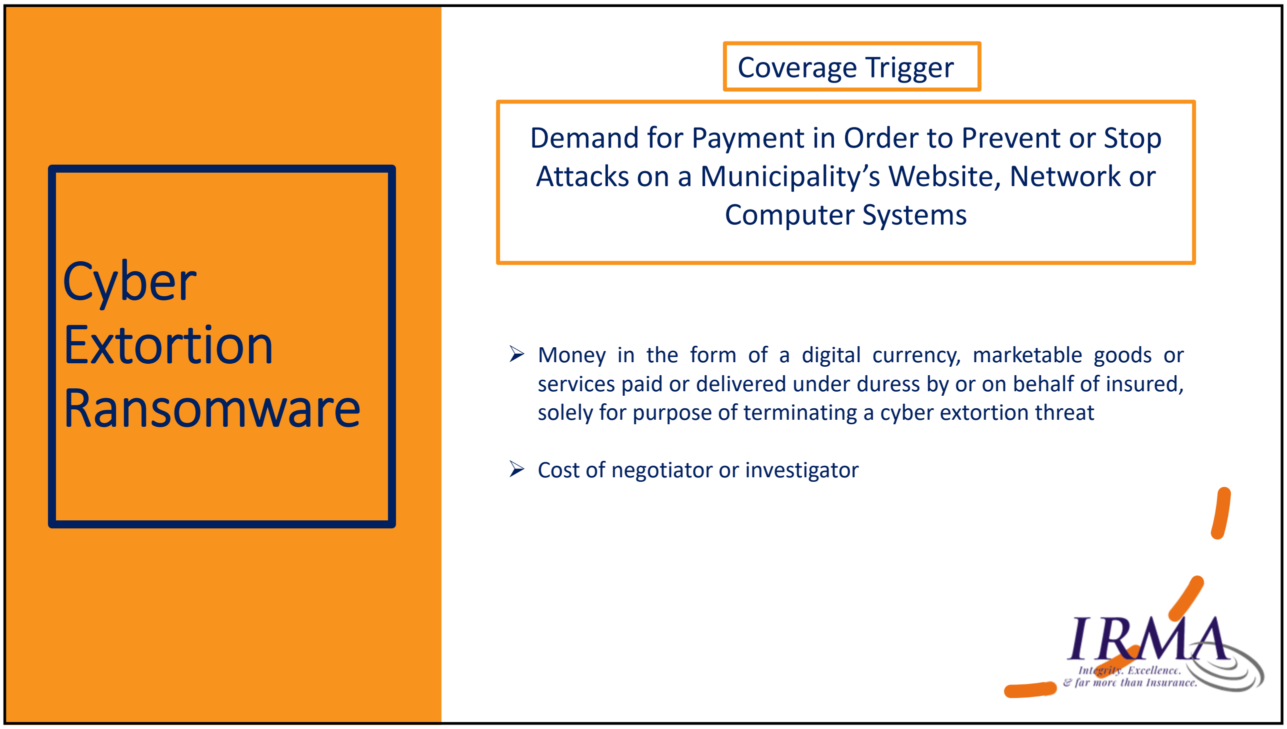
- Breach of 3rd Party Business Information
- Unintended propagation or forwarding malware
- Unintended abetting or a denial of service attack

Electronic Medial Liability

- Infringement of copyright, title, trademark, service mark
- Unintended Defamation
- Violation of Right of Privacy

IRMA
Integrity. Excellence.
& far more than Insurance.

45



Cyber Extortion Ransomware

Coverage Trigger

Demand for Payment in Order to Prevent or Stop Attacks on a Municipality's Website, Network or Computer Systems

- Money in the form of a digital currency, marketable goods or services paid or delivered under duress by or on behalf of insured, solely for purpose of terminating a cyber extortion threat
- Cost of negotiator or investigator

IRMA
Integrity. Excellence.
& far more than Insurance.

46

Computer Attack

Coverage Trigger

Direct Physical Loss or Damage to EDP and EDP Data and Media

- Data Restoration Costs
- Data Recreation Costs
- System Restoration Costs to Pre-attack level
- Loss of Business
- Extended Income Recovery
- Public Relations Services

47

IRMA's Cyber Declarations

CYBER SUITE COVERAGE
SUPPLEMENTAL DECLARATIONS
November 1, 2020 to November 1, 2021

Annual Aggregate Limit per Member:	$1,000,000
Deductible Per Occurrence:	$ 10,000
DATA COMPROMISE RESPONSE EXPENSES	Included
Sublimits Per Occurrence	
Forensic IT Review:	$500,000
Legal Review:	$500,000
Public Relations:	$5,000
Regulatory Fines and Penalties:	$500,000
PCI Fines and Penalties:	$500,000
COMPUTER ATTACK	Included
Sublimits Per Occurrence	
Loss of Business:	$500,000
Public Relations:	$5,000
CYBER EXTORTION	Included
Sublimit Per Occurrence:	$25,000**
MISDIRECTED PAYMENT FRAUD	Included
Sublimit Per Occurrence:	$25,000
COMPUTER FRAUD	Included
Sublimit Per Occurrence:	$25,000
DATA COMPROMISE LIABILITY	Included
NETWORK SECURITY LIABILITY	Included
ELECTRONIC MEDIA LIABILITY	Included

**IRMA provides excess cyber extortion coverage of $75,000 over the HSB sublimit.

48

What To Do if You Experience a Cyber Attack

Initial Steps

- Take the necessary steps to prevent further damage
- Locate the last system backup
- Save everything
- Report the claim to IRMA
  - Complete the Notice of Loss Form
  - Complete the Cyber Incident Questionnaire
- Notify Law Enforcement
- Evaluate whether personal identifying information, personal health information or personal sensitive information in your care, custody or control has been exposed

IRMA
Integrity. Excellence.
& far more than Insurance.

49

What To Do if You Experience a Cyber Attack

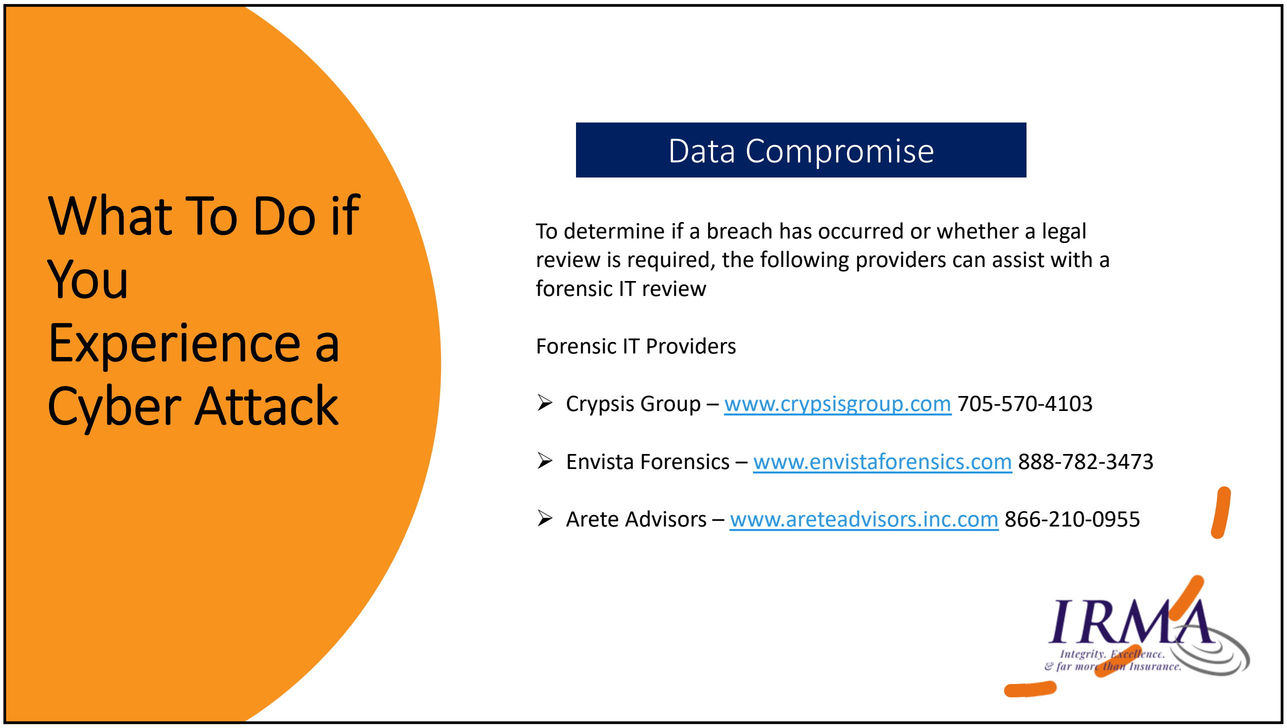
Ransomware Attack

Determine if your IT provider will restore the systems. If not, the following providers can assist with ransom negotiations and data restoration process:

- Coveware – www.coveware.com 203-442-4050
- Cyrpsis Group – www.crypsisgroup.com 705-570-4103
- Kivu Consulting – www.kivuconsulting.com 415-524-7320

IRMA
Integrity. Excellence.
& far more than Insurance.

50



What To Do if You Experience a Cyber Attack

Data Compromise

To determine if a breach has occurred or whether a legal review is required, the following providers can assist with a forensic IT review

Forensic IT Providers

- Crypsis Group – www.crypsisgroup.com 705-570-4103
- Envista Forensics – www.envistaforensics.com 888-782-3473
- Arete Advisors – www.areteadvisors.inc.com 866-210-0955

IRMA
Integrity. Excellence.
& far more than Insurance.

51

What To Do if You Experience a Cyber Attack

Legal Review

A legal review may be necessary to determine if there is a need to respond to any State Laws or Federal Regulations or if there is an obligation to provide credit monitoring

Legal Firms

- Lewis Brisbois Bisgaard Smith – www.lewisbrisbois.com 844-312-3961
- Jackson Lewis – www.jacksonlewis.com 844-544-5296
- Marshall Dennehey – www.marshalldennehey.com 800-220-3308

Credit Monitoring/Notifications Services

- ID Experts – www.idexpertscorp.com 800-298-7558
- Equip – www.equipglobal.com
- Experian – www.Experian.com 714-830-7000

IRMA
Integrity. Excellence.
& far more than Insurance.

52

What To Do if You Experience a Cyber Attack

Claim Process

- Notice of Loss given to HSB and IRMA
- IRMA opens claim
- HSB adjusts claim
  - Member submits paid bills to HSB for approval
  - HSB does coverage review
  - Approval and payment sent to IRMA
  - IRMA reimburses member through IRMA claim
- $10,000 Deductible

IRMA
Integrity. Excellence.
& far more than Insurance.

53

Final Thoughts

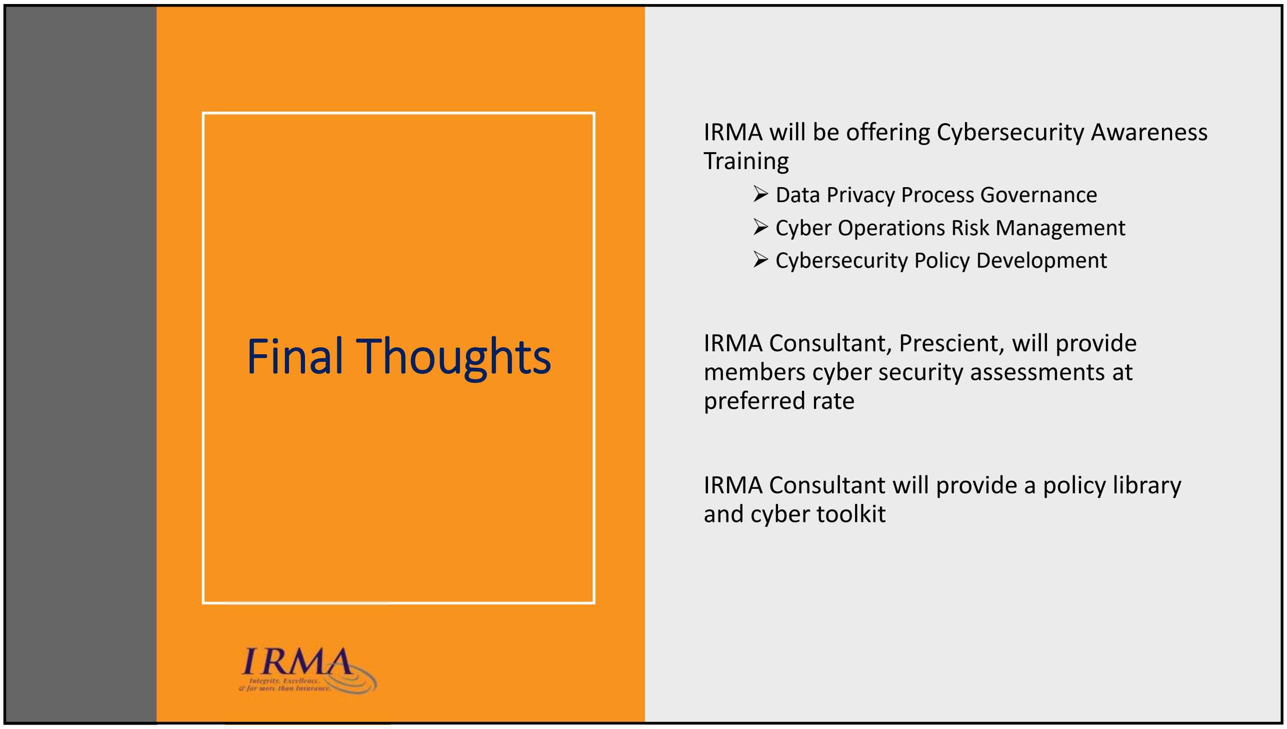
Basic cybersecurity best practices:

- Keep software up to date
- Run up-to-date antivirus software
- Use strong passwords
- Change default usernames and passwords
- Implement multi-factor authentication
- Install a firewall
- Be suspicious of unexpected emails
- Require employees to complete regular training

- Back up system is critical to avoid paying ransom
- Dedicate resources to cyber security

IRMA
Integrity. Excellence.
& far more than Insurance.

54



Final Thoughts

IRMA will be offering Cybersecurity Awareness Training

- ➢ Data Privacy Process Governance
- ➢ Cyber Operations Risk Management
- ➢ Cybersecurity Policy Development

IRMA Consultant, Prescient, will provide members cyber security assessments at preferred rate

IRMA Consultant will provide a policy library and cyber toolkit

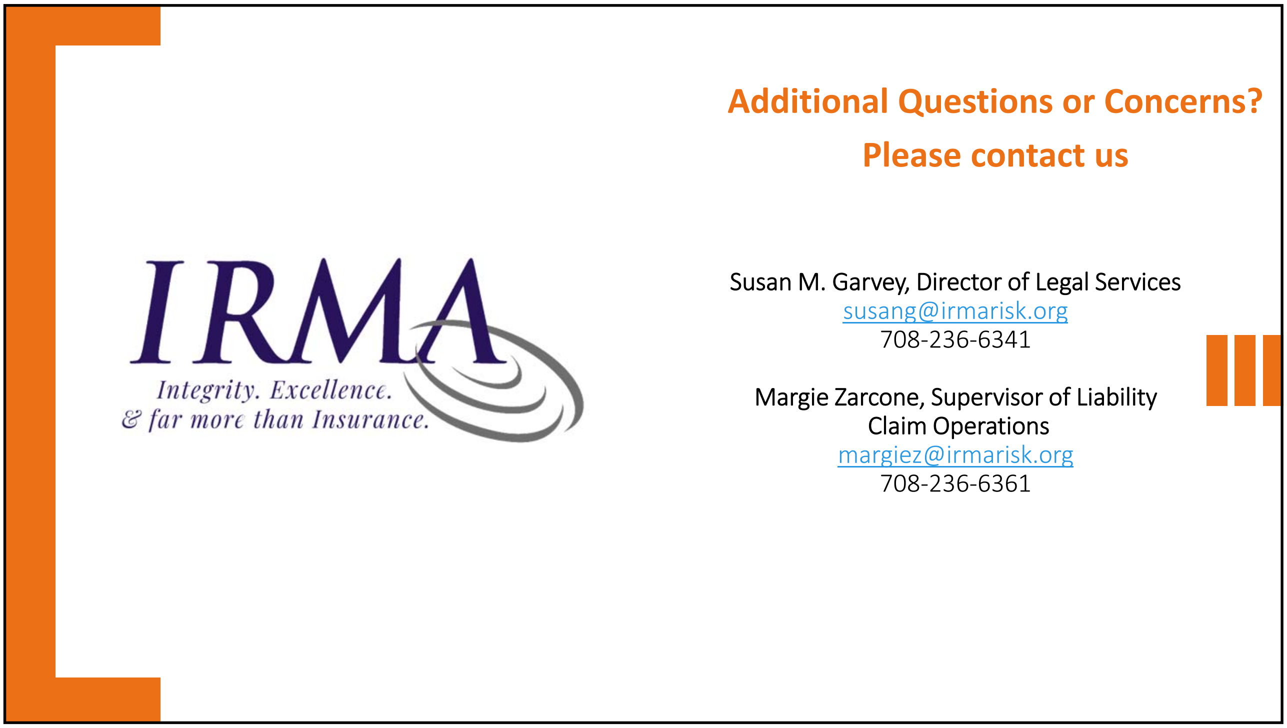
IRMA Integrity. Excellence. & far more than Insurance.

55

IRMA Integrity. Excellence. & far more than Insurance.

Questions?

56



IRMA

Integrity. Excellence.
& far more than Insurance.

Additional Questions or Concerns?
Please contact us

Susan M. Garvey, Director of Legal Services
susang@irmarisk.org
708-236-6341

Margie Zarcone, Supervisor of Liability
Claim Operations
margiez@irmarisk.org
708-236-6361

57