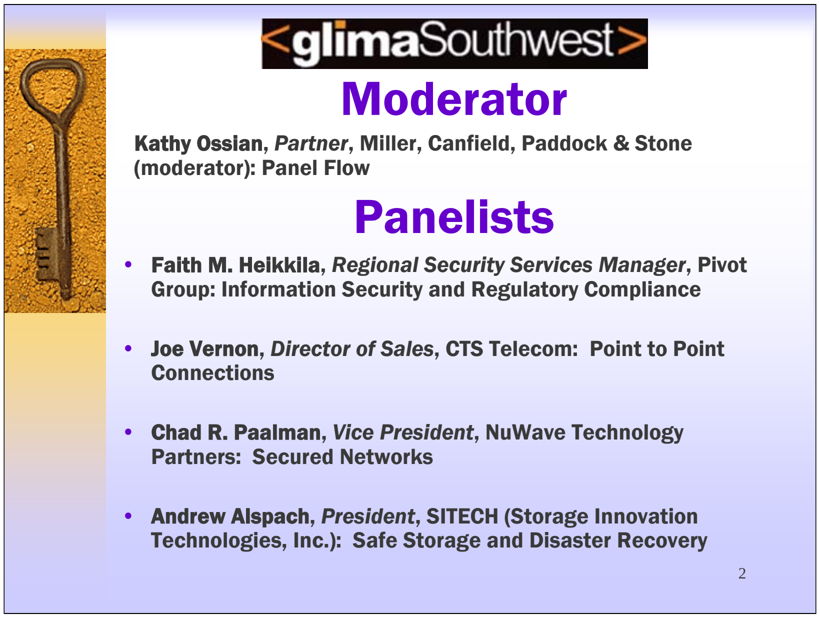
glimaSouthwest

Shedding Light on IT Security

Panel Discussion

May 24, 2007



glimaSouthwest

Moderator

Kathy Ossian, ***Partner***, **Miller, Canfield, Paddock & Stone (moderator): Panel Flow**

Panelists

- **Faith M. Heikkila**, ***Regional Security Services Manager***, **Pivot Group: Information Security and Regulatory Compliance**
- **Joe Vernon**, ***Director of Sales***, **CTS Telecom: Point to Point Connections**
- **Chad R. Paalman**, ***Vice President***, **NuWave Technology Partners: Secured Networks**
- **Andrew Alspach**, ***President***, **SITECH (Storage Innovation Technologies, Inc.): Safe Storage and Disaster Recovery**

2

Faith M. Heikkila

•glimaSouthwest Board member

•Regional Security Services Manager for the Pivot Group Great Lakes office here in Kalamazoo

•Ph.D. Candidate in Information Systems specializing in Information Assurance

•Previously a legal assistant for 18 years and the CIS Chairperson at Davenport GR

Published articles on:

•Secure telecommunications

•New Federal Rules of Civil Procedure E-Discovery rules

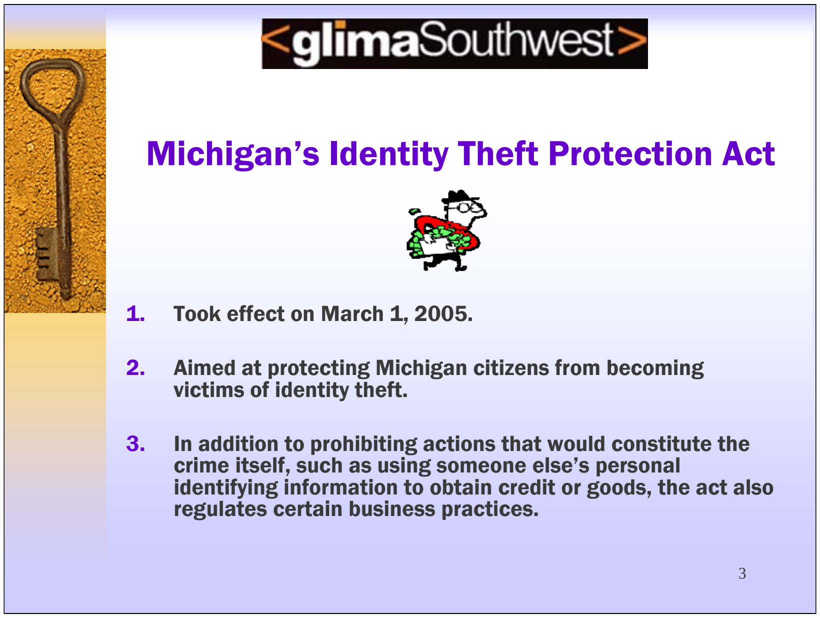
•Information security assessments

•"Encryption: Security considerations for portable and removable media" coming out at the end of this summer in the *IEEE Security & Privacy* magazine

Speaking engagements:

•Recently a SecureWorld Expo Chicago speaker on encryption and e-discovery

•Presentations at iConect Application Service Provider Conference and Information Systems Security Association (ISSA) in Grand Rapids on security issues and the new e-discovery rules and the Role of IT

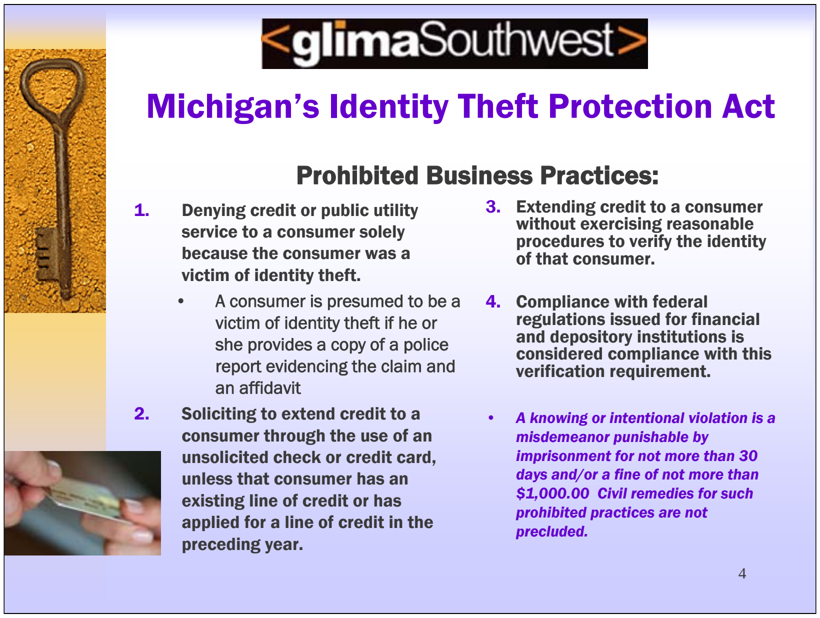


glimaSouthwest

Michigan's Identity Theft Protection Act

1. Took effect on March 1, 2005.
2. Aimed at protecting Michigan citizens from becoming victims of identity theft.
3. In addition to prohibiting actions that would constitute the crime itself, such as using someone else's personal identifying information to obtain credit or goods, the act also regulates certain business practices.

3



glimaSouthwest

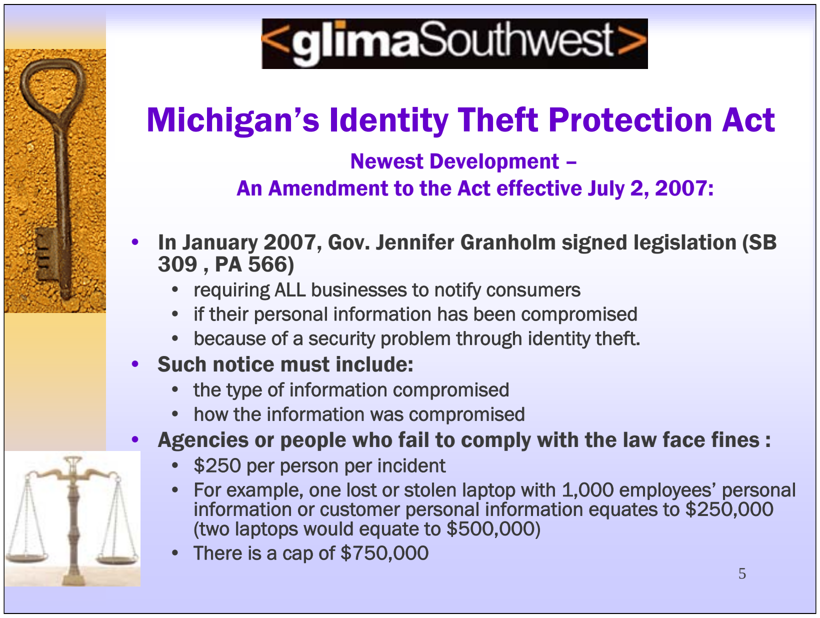
Michigan's Identity Theft Protection Act

Prohibited Business Practices:

1. **Denying credit or public utility service to a consumer solely because the consumer was a victim of identity theft.**
   - A consumer is presumed to be a victim of identity theft if he or she provides a copy of a police report evidencing the claim and an affidavit
2. **Soliciting to extend credit to a consumer through the use of an unsolicited check or credit card, unless that consumer has an existing line of credit or has applied for a line of credit in the preceding year.**
3. **Extending credit to a consumer without exercising reasonable procedures to verify the identity of that consumer.**
4. **Compliance with federal regulations issued for financial and depository institutions is considered compliance with this verification requirement.**

- ***A knowing or intentional violation is a misdemeanor punishable by imprisonment for not more than 30 days and/or a fine of not more than $1,000.00 Civil remedies for such prohibited practices are not precluded.***

4



<glimaSouthwest>

Michigan's Identity Theft Protection Act

Newest Development –
An Amendment to the Act effective July 2, 2007:

- **In January 2007, Gov. Jennifer Granholm signed legislation (SB 309 , PA 566)**
  - requiring ALL businesses to notify consumers
  - if their personal information has been compromised
  - because of a security problem through identity theft.
- **Such notice must include:**
  - the type of information compromised
  - how the information was compromised
- **Agencies or people who fail to comply with the law face fines :**
  - $250 per person per incident
  - For example, one lost or stolen laptop with 1,000 employees' personal information or customer personal information equates to $250,000 (two laptops would equate to $500,000)
  - There is a cap of $750,000

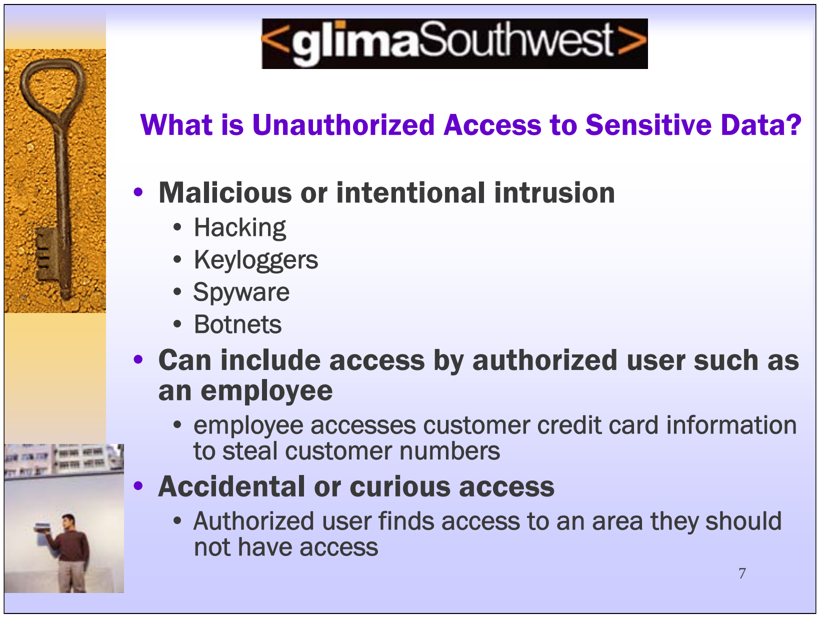
5

<glimaSouthwest>

Personal information constitutes:

- **First name or first initial and last name <u>PLUS</u>:**
  - Social Security Number
  - Financial account number
    - credit cards
    - debit cards
    - access codes
  - Driver's license number
  - State ID number

6

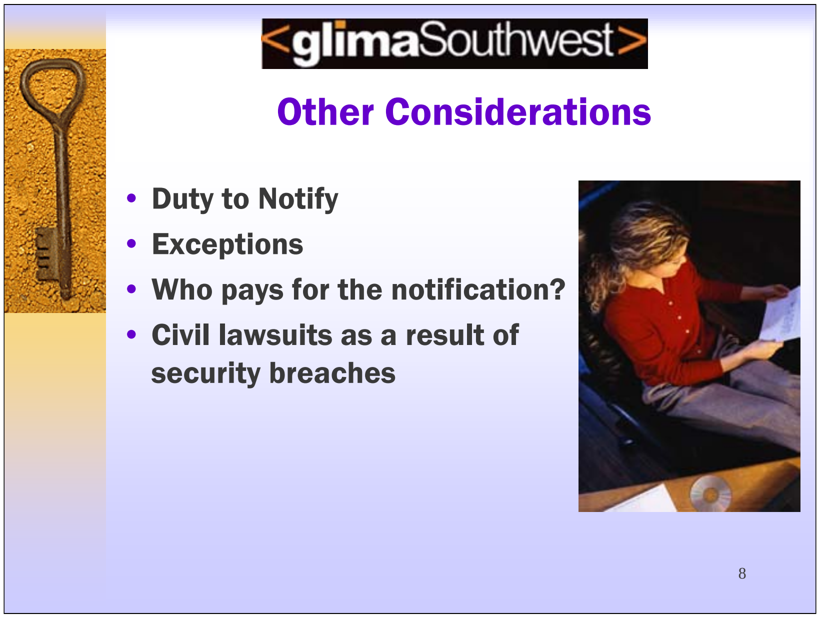


<glimaSouthwest>

What is Unauthorized Access to Sensitive Data?

- **Malicious or intentional intrusion**
  - Hacking
  - Keyloggers
  - Spyware
  - Botnets
- **Can include access by authorized user such as an employee**
  - employee accesses customer credit card information to steal customer numbers
- **Accidental or curious access**
  - Authorized user finds access to an area they should not have access

7



<glimaSouthwest>

Other Considerations

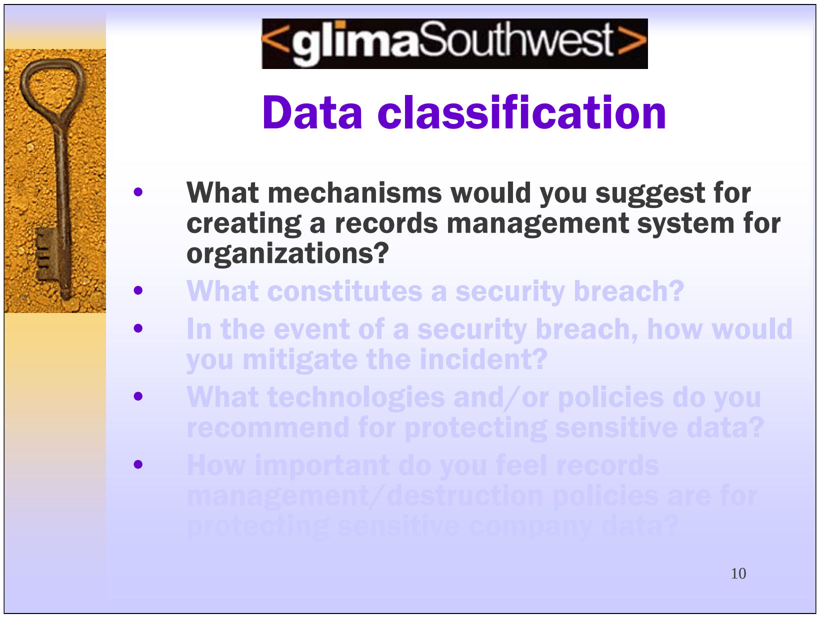
- Duty to Notify
- Exceptions
- Who pays for the notification?
- Civil lawsuits as a result of security breaches

8

<glimaSouthwest>

Panel Questions

9



<glimaSouthwest>

Data classification

- What mechanisms would you suggest for creating a records management system for organizations?
- What constitutes a security breach?
- In the event of a security breach, how would you mitigate the incident?
- What technologies and/or policies do you recommend for protecting sensitive data?
- How important do you feel records management/destruction policies are for protecting sensitive company data?

10

What mechanisms would you suggest for creating a records management system for organizations?

Document audit, classification system that work for you and your industry, policies, technology, training, monitoring & enforcement.

Data classification includes a records management system that implements Administrative Protections.

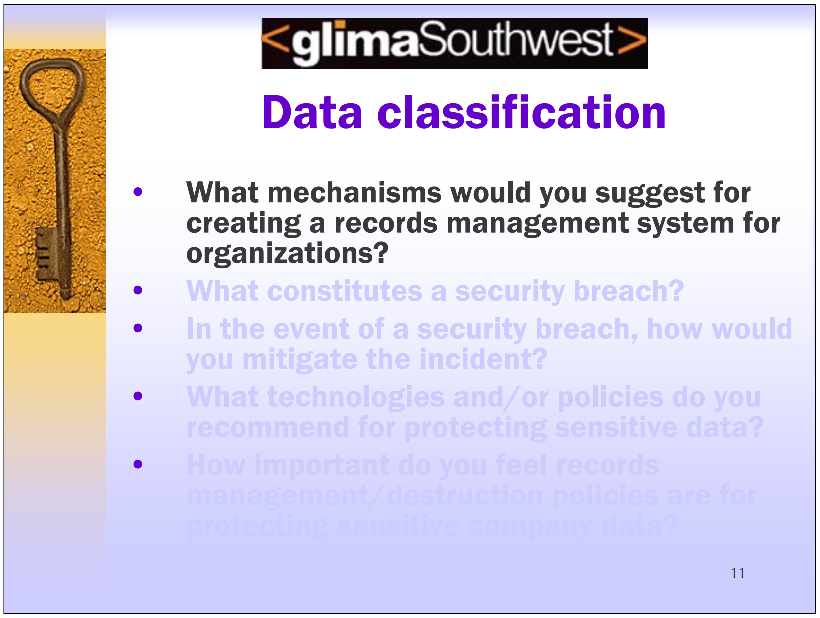
Critical to use a classification system that works for your company – Document classification

Military classifies:

- **Unclassified**
- **Confidential**
- **Secret**
- **Top Secret**

Organizations classifies as:

- **<u>Public domain</u> – one level**
- **<u>Internal Use</u> – not sensitive but not public**
- **<u>Confidential</u> – limit access to need-to-know**
- **<u>Strictly Confidential</u> – only top management can access**



<glimaSouthwest>

Data classification

- What mechanisms would you suggest for creating a records management system for organizations?
- What constitutes a security breach?
- In the event of a security breach, how would you mitigate the incident?
- What technologies and/or policies do you recommend for protecting sensitive data?
- How important do you feel records management/destruction policies are for protecting sensitive company data?

11

What mechanisms would you suggest for creating a records management system for organizations?

Most importantly identify:

- **Information that must be secured and where it is stored**
- **Data no longer needed and should be discarded**
- **Establish data owners responsible for keeping data secure**
- **Identify employees who require access to the records**
- **Implement Access controls to limit access**
- **Create a training program to educate users as to how to protect personal identifiable information.**

It is important to know where sensitive information resides:

Abe Usher of Sharp Ideas, created an application called Slurp.exe to demonstrate the need to protect your sensitive information from being downloaded onto portable and removable media devices.

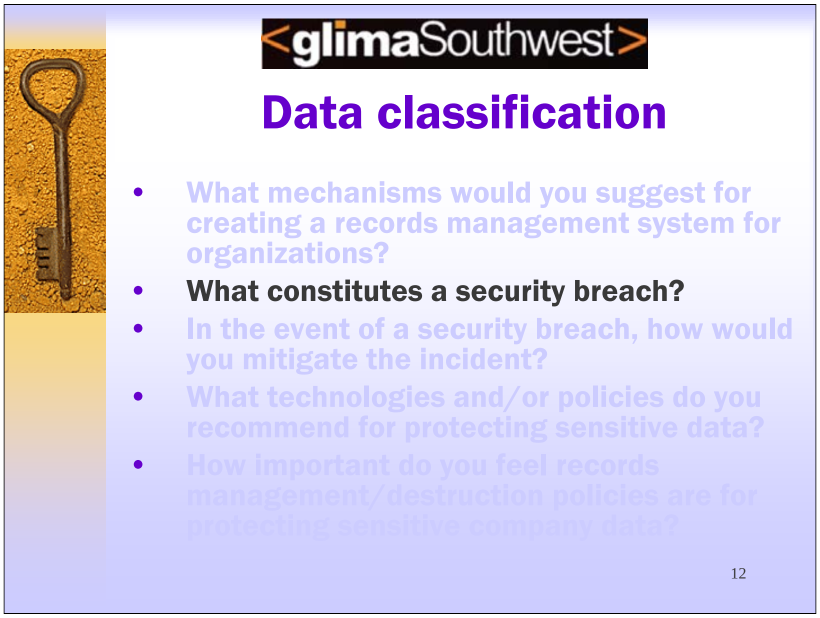
It is estimated that this Pod Slurping can assist with the download of more than 20,000 files per hour.

Usher, "Sharp Ideas' Slurp Audit Exposes Threat of Portable Storage Devices for Corporate Data Theft," January 25, 2006, http://sharp-ideas.net/ideas/?p=16.

Kharif, "Pod Slurping to Threaten Security," *Business Week Online*, July 26, 2005, http://www.businessweek.com/the_thread/techbeat/archives/2005/07/pod_slurping_to.html?chan=search.

Laptop, USB drives lost – what was on it? Was it encrypted?

It is extremely important to know where sensitive data resides, whether it be on a hard drive, servers, laptops, backup tapes, or USB drives.



<glimaSouthwest>

Data classification

- What mechanisms would you suggest for creating a records management system for organizations?
- What constitutes a security breach?
- In the event of a security breach, how would you mitigate the incident?
- What technologies and/or policies do you recommend for protecting sensitive data?
- How important do you feel records management/destruction policies are for protecting sensitive company data?

12

What constitutes a security breach?

Losing or exposing confidential data

36 States in the US have a security breach law

Michigan was the last of the Great Lakes states to adopt one.

Started in California with SB 1386

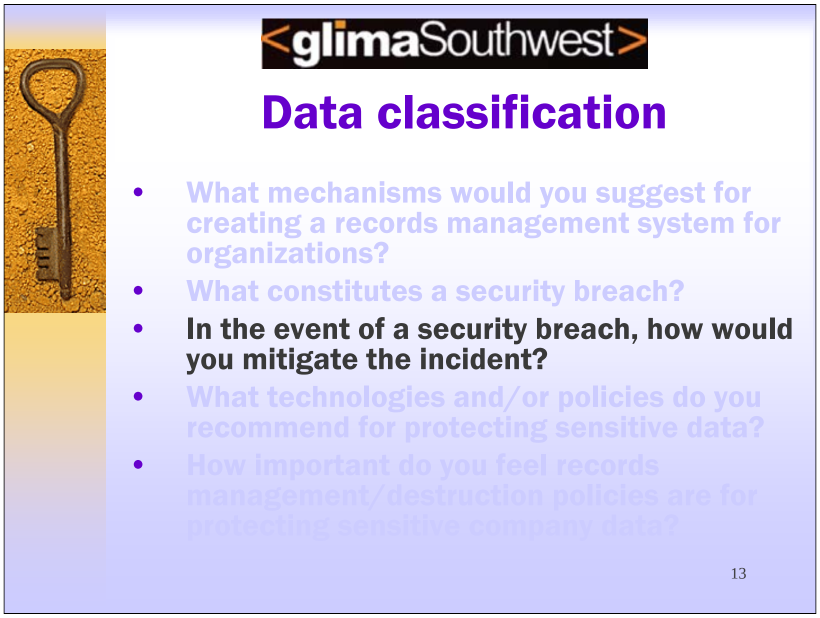
- **European Union (EU) Data Directive does not allow for the collection of personal information without the opt-in of its citizens**
- **NWA collected Frequent Flyer information in France. Under the EU Directive, this information is not allowed to be sent over to the US with a Safe Harbor agreement outlining how it will be protected. NWA was going to send it anyway; until France said they would not allow any NWA planes to land in France if they did transmit it to their US offices.**
- **You must know what privacy laws apply to your business.**

Site Recent Incidents = VA laptops, TJ Max, Cost them $26 Million with estimates of $8 billion when it is all over

Civil suits filed by banks requesting $10 million in damages - wanting TJ Max to repay their expenses for reissuing credit cards and notification costs

Triggers:

- **Must figure out what data was disclosed.**
- **To whom was it disclosed?**
- **How was it disclosed?**
- **In what format was it disclosed?**
- **How useful is the disclosed data to the recipient?**
- **In what state does the subject of the disclosed data reside?**
- **If lost data is encrypted = no security breach under most privacy laws.**
- **If a 3rd party is involved, it becomes more difficult to determine whether a security breach has been triggered.**
- **It would behoove you to discuss it with your Attorney.**



glimaSouthwest

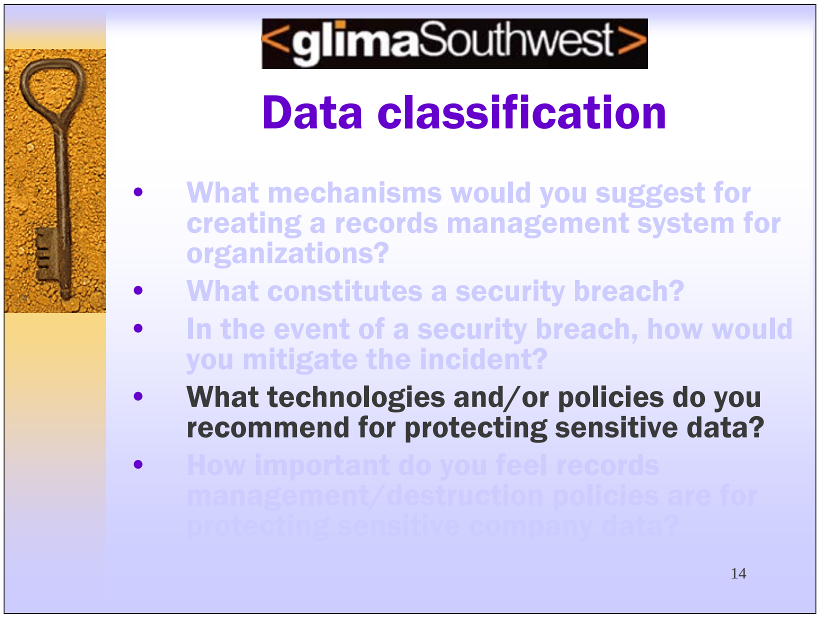
Data classification

- What mechanisms would you suggest for creating a records management system for organizations?
- What constitutes a security breach?
- In the event of a security breach, how would you mitigate the incident?
- What technologies and/or policies do you recommend for protecting sensitive data?
- How important do you feel records management/destruction policies are for protecting sensitive company data?

In the event of a security breach, how would you mitigate the incident?

Contain, eradicate, report, and build protection, repair, and test

1. **Investigate the incident and see if an incident has been declared based on the triggers**
2. **Assemble the Incident Response Team**
3. **Unplug the computer from the network – do not reboot the computer in order to preserve forensic evidence of how the incident occurred.**
4. **If the network has been compromised, take it offline until you can assure that being online is not producing more damage.**
5. **Investigate**



<glimaSouthwest>

Data classification

- What mechanisms would you suggest for creating a records management system for organizations?
- What constitutes a security breach?
- In the event of a security breach, how would you mitigate the incident?
- What technologies and/or policies do you recommend for protecting sensitive data?
- How important do you feel records management/destruction policies are for protecting sensitive company data?

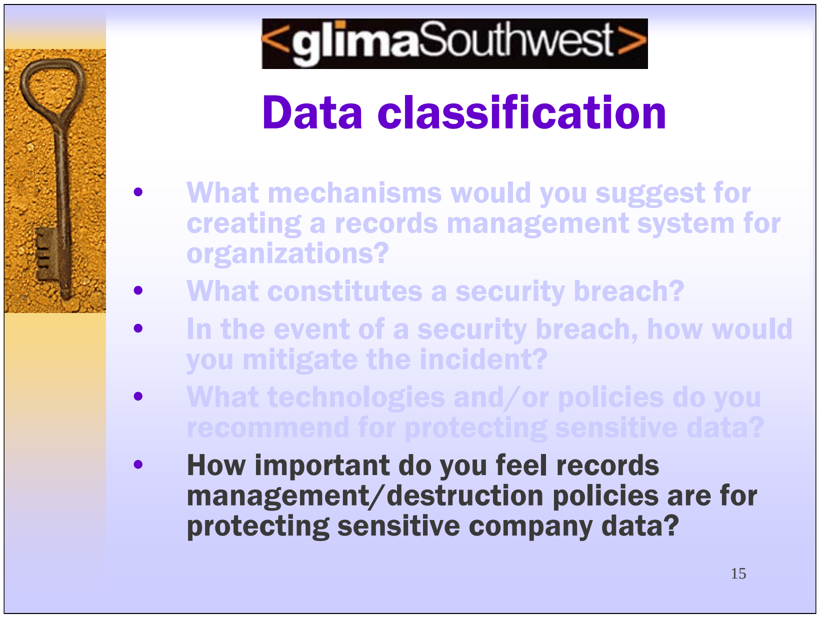
14

What technologies and/or policies do you recommend for protecting sensitive data?

Technologies: IDS/IPS, Encryption, Passwords, authentication, DMZ

1. **Monitoring software**
2. **Handling of personal information – disposal procedures**
3. **Banks and CUs – Confidential Member Information**
4. **No downloading of CMI at home**
5. **Do not leave CMI in open areas when not at desk**
6. **Termination policies**

Policies: acceptable use, protection, incident response, password, user access & credentialing



<glimaSouthwest>

Data classification

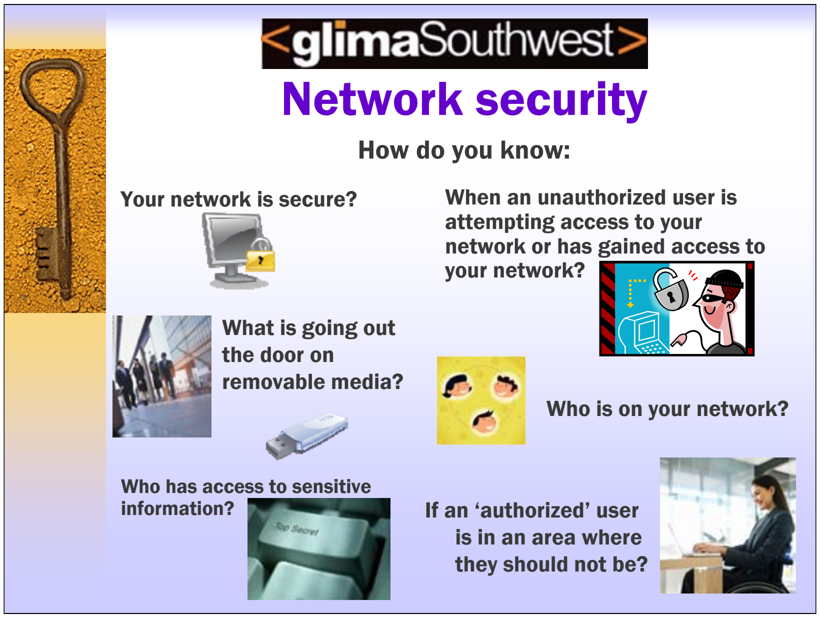
- What mechanisms would you suggest for creating a records management system for organizations?
- What constitutes a security breach?
- In the event of a security breach, how would you mitigate the incident?
- What technologies and/or policies do you recommend for protecting sensitive data?
- **How important do you feel records management/destruction policies are for protecting sensitive company data?**

15

How important do you feel records management/destruction policies are for protecting sensitive company data?

Records management is extremely important, especially in light of the new Federal Rules of Civil Procedures (FRCP) e-discovery rules

Destruction of equipment and sensitive data – regulatory compliance requirement in most instances.



<glimaSouthwest>

Network security

How do you know:

Your network is secure?

When an unauthorized user is attempting access to your network or has gained access to your network?

What is going out the door on removable media?

Who is on your network?

Who has access to sensitive information?

If an 'authorized' user is in an area where they should not be?

Your network is secure?

Who is on your network?

- **Regular testing & auditing**
- **Perform an external and internal vulnerability assessment.**
- **Discover where your network is vulnerable and mitigate the vulnerabilities.**

When an unauthorized user is attempting access to your network or has gained access to your network?

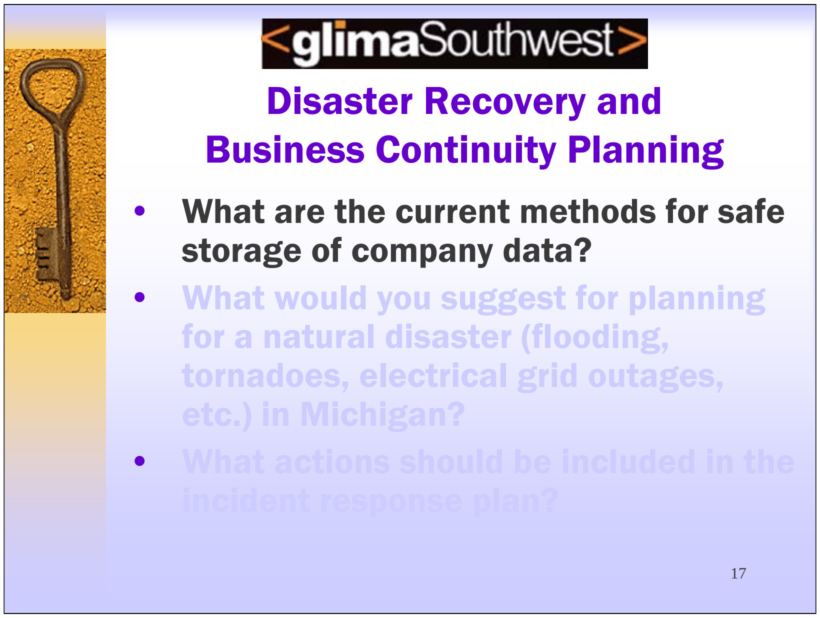
- **IDS/IPS**
- **Alerts of activity**

Who has access to sensitive information?

If an 'authorized' user is in an area where they should not be?

What is going out the door on removable media?

- **Monitoring software such as Tablus or Vontu**
- **If credit card number, SSN, account number is detected in e-mail, the monitoring software will stop the transmission**
- **Send the employee an e-mail indicating whether they are aware that they are violating company policy and possibly should privacy laws by sending this personal identifiable information out unencrypted?**
- **Usually after two weeks of installing this type of software, there is an 85% drop in these types of e-mails going out.**



<glimaSouthwest>

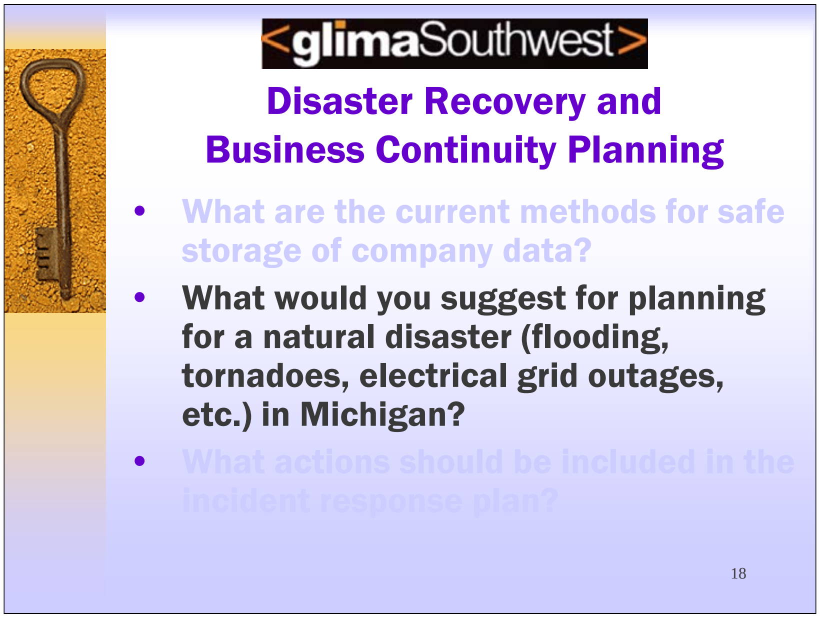
Disaster Recovery and Business Continuity Planning

- What are the current methods for safe storage of company data?
- What would you suggest for planning for a natural disaster (flooding, tornadoes, electrical grid outages, etc.) in Michigan?
- What actions should be included in the incident response plan?

17

What are the current methods for safe storage of company data?

- **Encryption, password protect, policies, training, lock & key, physical monitoring & security**
- **Encrypted drives on hard drive used as the default drive – users are unaware of encrypted drive – seamless to them.**
- **Physical security**
- **Placing backup tapes in a safe storage place – protected from natural disasters.**



<glimaSouthwest>

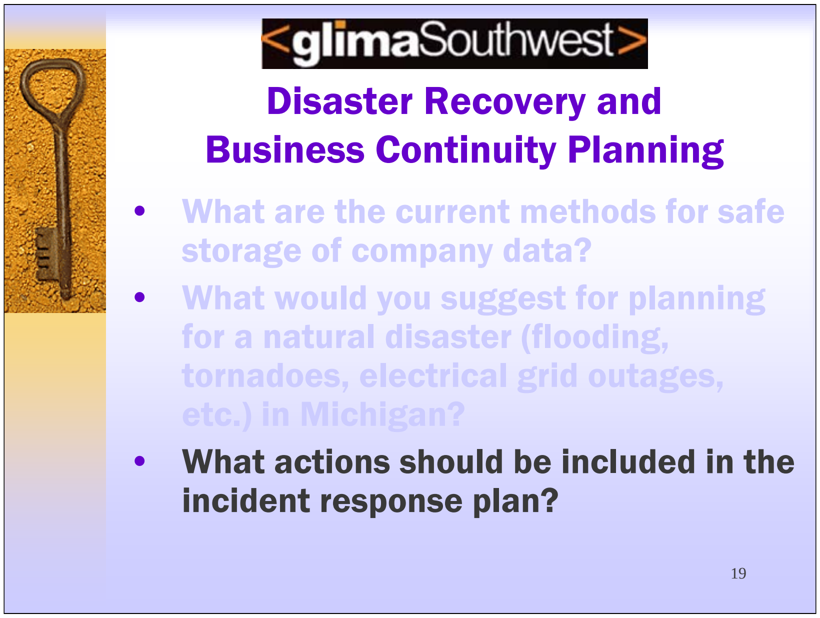
Disaster Recovery and Business Continuity Planning

- What are the current methods for safe storage of company data?
- What would you suggest for planning for a natural disaster (flooding, tornadoes, electrical grid outages, etc.) in Michigan?
- What actions should be included in the incident response plan?

18

What would you suggest for planning for a natural disaster (flooding, tornadoes, electrical grid outages, etc.) in Michigan?

- **Ice, snow, tornado, Business continuity & Recovery Plan, Test it regularly, offsite hot site, telecommunication plan.**
- **Hurricane Katrina provided us with many great lessons with regard to disaster planning.**
- **Redundant systems in remote locations – 9/11 Appalachian Mountains**
- **Backups in locations outside of same geographic region.**



<glimaSouthwest>

Disaster Recovery and Business Continuity Planning

- What are the current methods for safe storage of company data?
- What would you suggest for planning for a natural disaster (flooding, tornadoes, electrical grid outages, etc.) in Michigan?
- What actions should be included in the incident response plan?

19

What actions should be included in the incident response plan?

- **Check our website or SANS**
- **Creation of an Incident Response Team – Develop team *before* an incident occurs**
- **Communication list exchange and telephone chain**
- **Layered Response**
- **First Responders**
- **Incident Command Center**
- **Field Responders – forensic experts to image and interpret incident**
- **Tools to use – EnCase, NetForensics**

Incident Response Plan should include:

1. **Interdiction – Relationship with ISP is important in order to terminate connection via ISP backbone routers**
2. **Containment – if necessary, terminate Internet connection until attack subsides, isolate vulnerable/critical assets temporarily**
3. **Recovery – analyze damage and respond**
4. **Analysis – formal incident post mortem at completion of incident**

glimaSouthwest

Best Practices and Recommendations

- What would you recommend as the best practices for safeguarding data at rest and in transit?
- What would you recommend as the best practices for safe disposal of computer equipment and electronic files?
- What happens after a security incident occurs?

20

What would you recommend as the best practices for safeguarding data at rest and in transit?

- **Encrypted servers for confidential information**
- **Encryption for removable media devices – authorize device, authenticate it, and log activity.**
- **Multiple levels of security or defense-in-depth (firewalls, anti-virus, anti-spyware, intrusion detection systems/intrusion prevention systems (IDS/IPS), etc.)**

- **Calgary study of laptop thefts concluded that physical security works if properly done – rarely recovered laptops**

From an encryption trend perspective, there are 3 evolving trends:

1. **Regulation Trend which is driving a**
2. **Technology Trend which is driving a**
3. **Culture trend.**

<glimaSouthwest>

Best Practices and Recommendations

- What would you recommend as the best practices for safeguarding data at rest and in transit?
- What would you recommend as the best practices for safe disposal of computer equipment and electronic files?
- What happens after a security incident occurs?

21

What would you recommend as the best practices for safe disposal of computer equipment and electronic files?

1. **Bonded services for the specific medium**
2. **Cross shredder for all paper documents**
3. **Shredder for hard drives**
4. **Electronic shredding (7 times rewrite) – McAfee and Norton have this capability**
5. **Escort the equipment to shredding company and oversee the destruction**

<glimaSouthwest>

Best Practices and Recommendations

- What would you recommend as the best practices for safeguarding data at rest and in transit?
- What would you recommend as the best practices for safe disposal of computer equipment and electronic files?
- **What happens after a security incident occurs?**

22

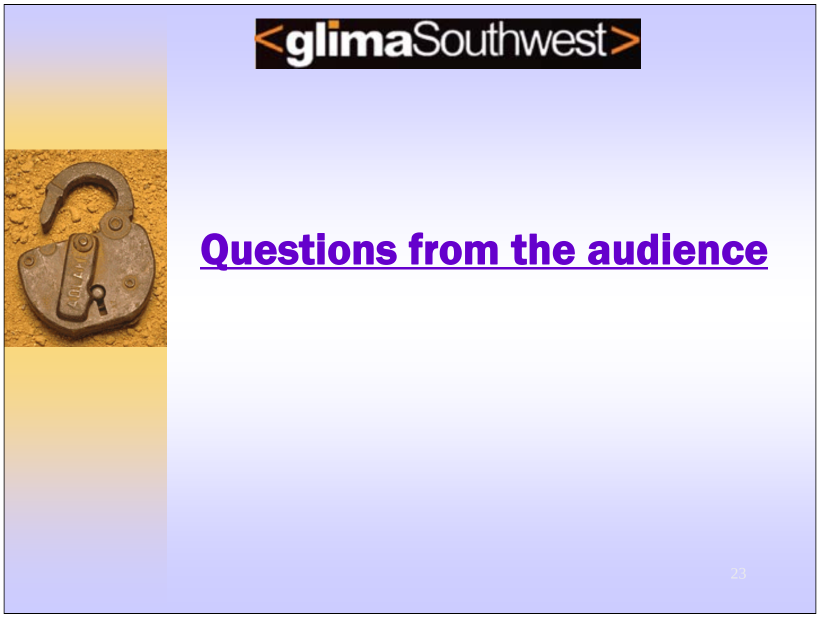
What happens after a security incident occurs?

Damage control, Secure the site, Stop & eradicate (interdict) the incident, Reporting, Post mortem, Fix the problem, Test the fix, Regulator & law enforcement inquisition,

Prepare for legal proceedings, Prepare for fines, fees, damages! Paranoia!

Good time to brush up your resume or ask for more money!

- **Stop the bleeding**
- **Forensics**
- **Identify how the breach happened**
- **Plug the hole**
- **Determine whether a notification is required – consult with attorney**
- **Response / notification of the incident or breach**
  1. **Interdiction – Relationship with ISP is important in order to terminate connection via ISP backbone routers**
  2. **Containment – if necessary, terminate Internet connection until attack subsides, isolate vulnerable/critical assets temporarily**
  3. **Recovery – analyze damage and respond**
  4. **Analysis – formal incident post mortem at completion of incident**



<glimaSouthwest>

Questions from the audience

23

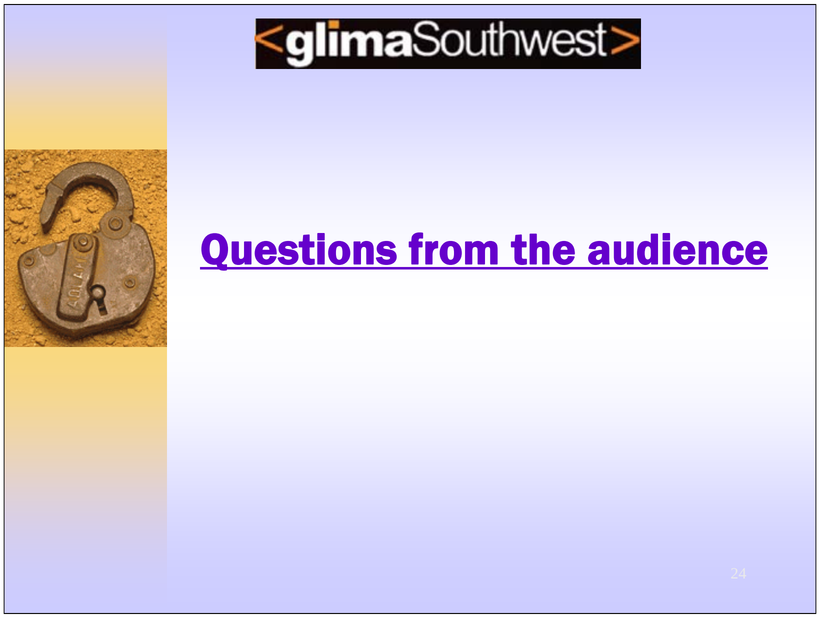
1. How do the laws affect benefit providers who require full SSN. Prefer to only give last 4 digits – but many won't accept this. What options do we have?
   - You can ask your insurance carrier to assign a unique number to your account rather than your Social Security Number. Then, when benefit providers require a number, this new unique number can be used. The issue, however, is that the patient will have to always remember what that number is in order to be able to get benefits.

2. Security in faxing vs. emailing? Differences? Who is liable if something is faxed and the receiving organization loses the information or it is stolen? If you can't feel comfortable emailing sensitive information, is the U.S. Post Office any better?

   Chad answered this one.

3. Should we require security breach policies **from** companies that come into our facility to set up or repair equipment? Such as AT&T, CTS, etc.

   Kathy answered this one.



<glimaSouthwest>

Questions from the audience

24

1. What about MAC's in a PC environment? MAC users tend to think they are invincible and don't think they could ever damage the network. We have 2 MAC users in a PC environment – is there anything I can do to protect the network?

   Chad answered this one.

   MACs have been getting hit hard lately with new vulnerabilities every day. There were 13 recent MAC security patches following up about 25 security patches in the first part of this year.

2. What do you think about remote access like logmein.com, gotoassist, etc.?

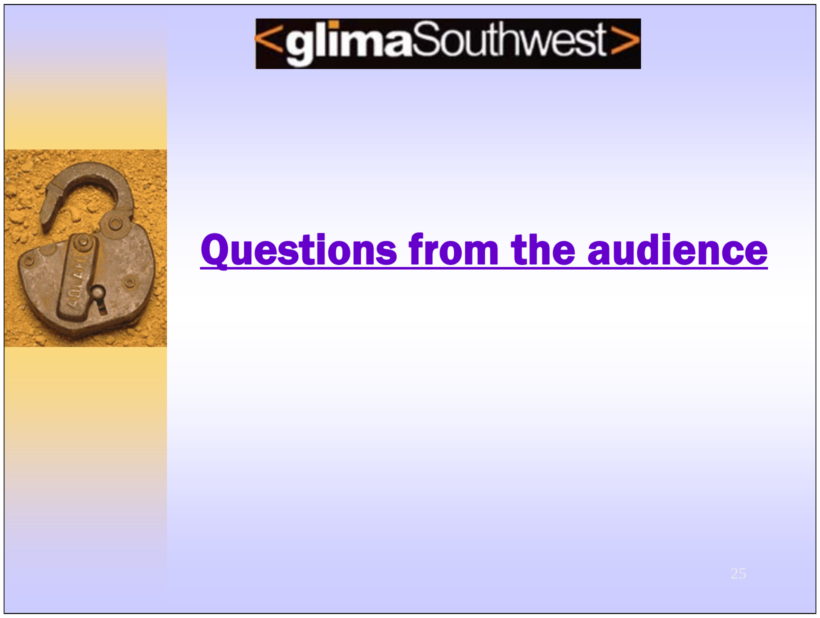
   Chad answered this one.

3. Why won't the Michigan law (a felony) against stealing (logging on to) another wireless service without permission stop (or prevent) problems.

   It is incredibly hard to prosecute these types of cases due to the fact that it is hard to prove precisely who is logging on to another's wireless service without permission.

4. Can you recommend any product that will erase a hard drive securely enough to avoid shredding them? Or so they could be re-used internally for less sensitive data?

   - The DoD has software that they use. Not sure what it is called. McAfee and Norton have the capabilities of shredding electronic files 7 times (the DoD standard). This would probably suffice your need for reuse of the machine internally.



<glimaSouthwest>

Questions from the audience

25

These questions were posed to Chad Paalman and Kathy Ossian (our moderator):

For Chad:

50% of back ups fail……. Why? How can you prevent a backup from failing?

For Kathy:

Many companies are outsourcing applications that involve private information and data protection: (European directive, Safe Harbor, etc.) What clause (in the ASP contract) can a company hiring an ASP use, to ensure the ASP has the proper technologies and policies?

<glimaSouthwest>

Closing Thoughts

CTS TELECOM, INC.
CLIMAX TELEPHONE COMPANY

PIVOTGROUP
Armed with Information Security Knowledge

MILLER CANFIELD
MILLER, CANFIELD, PADDOCK AND STONE, P.L.C.

NUWAVE
TECHNOLOGY PARTNERS

100 Years 1903-2003
Chamber
Kalamazoo Regional Chamber of Commerce

SITECH
Storage Innovation Technologies, Inc.

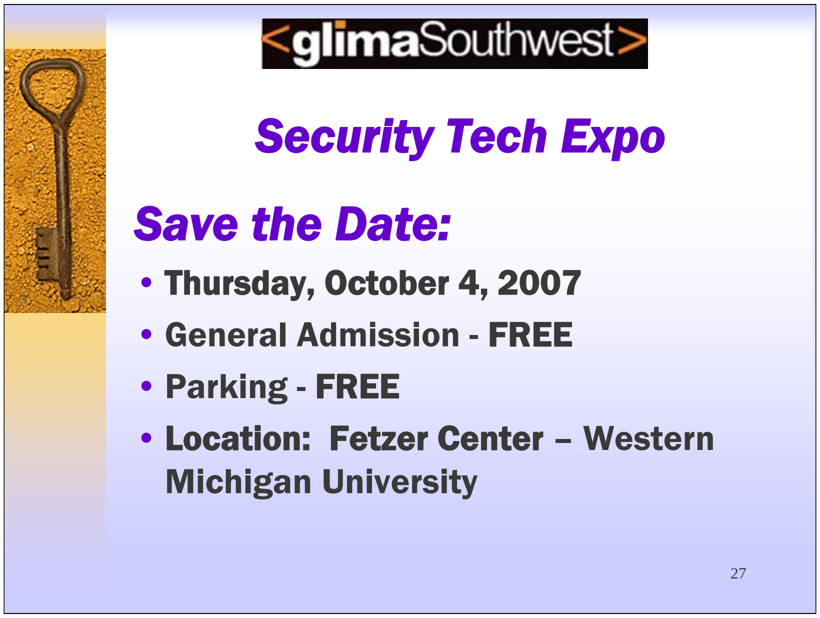
26

Closing Remarks

Remember it is NOT just a technology issue. Technology is only an enabler.

I would like to leave you with these take-aways on Data Privacy and Protection

1. **Know what Data you want to protect.**
2. **Implement a Culture, Policies, Procedures, and training around your risk strategy and tolerance.**
3. **Use technology to enable your data privacy and protection strategy, policies and procedures. And make sure it is easy to use.**
4. **Make sure you know when an incident has happened and know what to do when it happens.**
5. **Be familiar with appropriate laws and regulations so you are in compliance.**



<glimaSouthwest>

Security Tech Expo

Save the Date:

- **Thursday, October 4, 2007**
- **General Admission - FREE**
- **Parking - FREE**
- **Location: Fetzer Center – Western Michigan University**

27

The following is the current confirmed line up of speakers as of May 24, 2007:

•Lunch Keynote – Dan Lohrmann, CISO (Chief Information Security Officer) for the State of Michigan and President of InfraGard

•Tom Peltier of Peltier & Associates – nationally known expert and speaker on information security and author of numerous information security books.

•Brian Gawne of CTG

•Richard Rushing of Air Defense

•Tom Hines of Secure Matrix and President of the Michigan Homeland Security Consortium

•Jim Soenksen of Pivot Group

•Justin Peltier of Peltier & Associates (tentative)