Are Law Firms Spending Their Money on the Wrong Areas of IT Security?

Presented by
Rob Kleeger
Joseph Riccie

OM34
5/5/2018
3:00 PM
OM34: Are Law Firms Spending Their Money on the Wrong Areas of IT Security?

AGENDA

- Facts and Figures
- Why traditional perimeter-based security is not enough for cyberattacks
- Cybersecurity and the Law - compliance and risk aspects of the business of law.
- Cost of data breach
- What does it mean to migrate to the cloud?
- Understanding your third party provider network and risks
- Implementing best practices - what you can do internally
CYBERCRIME STATISTICS

- Nearly half of all cyberattacks are committed against small businesses.
- Cybersecurity Ventures predicts that a business will fall victim to a ransomware attack every 14 seconds by 2019, increasing from every 40 seconds in 2017.
- Ransomware damages are up 15X in the past 2 years.
- A global survey conducted by the Microsoft Digital Crimes Unit last year showed two out of three people experienced a tech support scam in the previous 12 months.
- 91% of attacks by sophisticated cybercriminals start through spear phishing emails.
- Cyber criminals are creating an average of around 1.4 million phishing websites every month with fake pages designed to mimic the company they’re spoofing.

Cybercrime Damages $6 Trillion By 2021

THE GOOD NEWS

Source: 2017/2018 Thales Data Threat Report
MOTIVATIONS FOR INCREASED SPENDING

Source: 2017/2018 Thales Data Threat Report

THE GOOD NEWS IN DETAIL

Source: 2017/2018 Thales Data Threat Report
So why have law firms traditionally been not as sophisticated in ensuring that they are protected from cyber risk?

The simple answer is that it costs a great deal of money to ensure cyber risk is controlled and most small and midsized law firms have not been particularly keen on investing in protecting against it.
TOP LAW FIRM TRENDS FOR 2018

2. These Boots are made for Walking!
3. The Great Cloud Migration: To migrate to the cloud or adopt a middle ground

PRIMARY REASONS FOR LAW FIRM CYBER SECURITY FAILURES

❖ **Common misconceptions.** Most lawyers understandably think of cyber security as an IT problem.

❖ **Traditional security strategies.** Most enterprise risk management tends to be specialized. The finance department handles financial risks. The legal department handles legal risks. The facilities department handles physical security risks. The IT department handles IT risks. **Digital risks span all of those various risks.**

❖ **Security risk factors: culture and enforcement.** There are certain behaviors and activities that correlate with the likelihood that there will be a breach. One is tolerance for inconvenience.

A truism, in information security, is that security and convenience are inversely related. You cannot have both!

One example is passwords. The longer they are, the harder it is for employees to memorize them.

❖ **Choice overload.** This is a term invented by Columbia Business School professor, Dr. Sheena Iyengar, whose research is around what drives consumers to buy. There is an “avalanche” of products in the information security field, especially for small and medium sized businesses.
Before migrating to the cloud – know your concerns

Source: 2017/2018 Thales Data Threat Report

<table>
<thead>
<tr>
<th>Top Cloud Security Concerns</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security breaches at the cloud provider</td>
<td></td>
</tr>
<tr>
<td>Shared infrastructure vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>Control of data location</td>
<td></td>
</tr>
<tr>
<td>Cloud Privileged user abuse</td>
<td></td>
</tr>
<tr>
<td>No data privacy policy/agreement</td>
<td></td>
</tr>
<tr>
<td>Custodianship of encryption keys</td>
<td></td>
</tr>
<tr>
<td>Visibility into security practices</td>
<td></td>
</tr>
<tr>
<td>Meeting compliance requirements</td>
<td></td>
</tr>
</tbody>
</table>

Is your data secure?
Cyber attackers will always find the course of least resistance into your protected networks and resources. And the research has shown the weakest point is almost always your users and their credentials.
WHY TRADITIONAL PERIMETER-BASED SECURITY IS NOT ENOUGH FOR CYBERATTACKS

Today’s enterprises are rapidly adopting cloud and hybrid infrastructure, new styles of working, and new ways of connecting remotely. Traditional network perimeters secure only the ingress and egress points of the company-managed network. Antivirus, next-gen firewalls, and VPN aren’t enough to thwart attacks on the modern enterprise. Modern enterprises need to define a new perimeter based on identity that secures company resources that are located anywhere; including users, devices, apps, data, and infrastructure.

3 REASONS A PERIMETER-BASED SECURITY APPROACH NO LONGER WORKS:

1: The definition of the perimeter is always changing.

2: The increased usage of end-to-end encryption decreases the value of a perimeter-based approach.

3: Internal-only activity (which never crosses any perimeter) is extremely valuable for your information security program.

The data you secure lives in the cloud, flowing through laptops and cellphones around the world. When information is everywhere, security must be everywhere, too!
MOVING BEYOND PERIMETER-BASED SECURITY

“CIOs have long considered the best defence to be a good offense when it comes to handling security threats, so the vast majority of time and money is spent building the perimeter security measures that keep the outsiders from getting into the network,” Former Websense CSO Jason Clark

• These strategies are 30-years-old and have to change.

• Perimeter is NOT dead, it’s just changed. It’s new and different.

• Authentication is be the new perimeter. The bad guys are going straight to the user and getting the data

A completely different way of thinking is required!

CYBERSECURITY AND THE LAW

When it comes to cybersecurity, attorneys from solo shops to BigLaw are grappling with tough issues.

Facing litigation after a phishing attack, attorneys contemplate the imperative to encrypt attorney-client communications.

The American Bar Association’s 2017 Legal Technology Survey Report found that 22 percent of respondents experienced a cyberattack or data breach at some point, an increase of 8 percentage points over the previous year.

Data breaches, a modern certainty like death and taxes, damage an attorney’s ability to provide zealous representation. Hacks can also cost large sums of money, as well as the profession’s own credibility.
Law Firms Are Unique, Right?

A Duty to Safeguard

Consequences of Breach

- Loss of client data.
- Business downtime/loss of billable hours.
- Hefty expenses for remediation/ hiring 3rd parties.
- Costs to replace hardware/software.
- Loss if important files and misc. data.

Employing & Increasing Safeguards Commonly Used in other Industries

- Programs and Policies - Protecting its data is establishing a comprehensive data security program. Plans need to identify, protect, detect, respond to and recover from cyber incidents. (i.e. Document or records management retention and destruction policy, Email usage policy, Internet use/computer usage policy, Social media and Cloud usage, Password usage, etc.)
- Assessments - Using security assessments conducted by independent third parties has been a growing security practice.
- Standards/Frameworks - Other industries use security standards and frameworks, like ISO 27001, the US National Institute of Standards and Technology (NIST) Cybersecurity Framework and SANS Critical Controls.
- Multi-Factor Authentication – offered in most enterprise solutions today.
- Encryption - Security professionals view encryption as a basic safeguard that should be widely deployed.
- Cybersecurity Insurance - Many general liability and malpractice polices do not cover security incidents or data breaches.

Client Confidences

- Law firms have heightened responsibility for maintaining the confidentiality of client information.
- Legal ethics rules, such as Rule 1.6, have underscored that lawyers are required to take reasonable efforts to prevent unauthorized access to client information.
  – To the extent that a client is damaged by a data breach occasioned by a lawyer’s revelation of confidences, disciplinary action is possible.
- A 2016 study by an insurance broker finds most leading legal malpractice insurers had a continuing increase in claims in excess of $50 million.
  – Half the insurers have had a LPL insurance claim arising from a cyber event, due to lost or stolen laptops, employee errors, hackers, and disgruntled employees.
- Law firms with clients in the financial services or healthcare industry have specific issues around the Gramm-Leach-Bliley Act and HIPAA.
2016: COST OF DATA BREACH

- Average Cost of Data breach - $158 per record
- Average Number of records per incident - 24,098
- Average Cost per incident - $3.8 Million

Total Cost of Incident

COST OF BREACHES

- $3,800 K

Incident Response Plan and Team
- Impact: $16
- Reduction by 10%

Total Cost of Incident
COST OF BREACHES

$3,800 K

$3,421 K

Extensive Use of Encryption
• Impact: $13
• Reduction by 8%

$313K

Incident Response Plan & Team

Total Cost of Incident

COST OF BREACHES

$3,800 K

$3,421 K

Extensive Use of Encryption
• Impact: $13
• Reduction by 8%

$313K

Incident Response Plan & Team

Total Cost of Incident

$3,108 K

$217K

Employee Training
• Impact: $9
• Reduction by 6%

$217K

Total Cost of Incident
COST OF BREACHES

Total Cost of Incident

CISO Appointed
- Impact: $7
- Reduction by 4%

$3,800 K
$3,421 K
$3,108 K
$2,890 K
$169 K

Incident Response Plan & Team
Extensive Use of Encryption
Employee Training

Board Level Involvement
- Impact: $6
- Reduction by 4%

$3,800 K
$3,421 K
$3,108 K
$2,890 K
$2,722 K
$145 K

Total Cost of Incident
Migrating to the Cloud – SaaS/IaaS/PaaS

CLOUD OPENING REMARKS

- The SaaS world continues to evolve and is by no means impenetrable.
- SaaS companies spend millions of dollars more than independent companies on security.
- SaaS companies comply with regulations or they are out of business.
- It is not a set it and forget it decision.
- You are still RESPONSIBLE!!
Poll: Why are you considering a move to the cloud?
### WHY ORGANIZATIONS CONSIDER THE CLOUD

<table>
<thead>
<tr>
<th>Feature</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved business agility</td>
<td>74%</td>
</tr>
<tr>
<td>Allows us to focus on more important projects</td>
<td>64%</td>
</tr>
<tr>
<td>Speed of deployment</td>
<td>62%</td>
</tr>
<tr>
<td>Lower overall costs</td>
<td>59%</td>
</tr>
<tr>
<td>Lack of IT staff to maintain the solution</td>
<td>49%</td>
</tr>
<tr>
<td>Change upfront costs to monthly payments</td>
<td>48%</td>
</tr>
</tbody>
</table>

### THE MICROSOFT CLOUD

- **A complete cloud designed for the enterprise**
- **Flexible, hyper-scale**
- **Open platform for development flexibility**
- **Rigorous security and compliance**
- **The right personal experience in a trusted cloud**
THE MICROSOFT CLOUD

PRODUCTIVITY

Office 365
- Documents
- Email, Calendar, Tasks
- Power BI
- Social/Collaboration

PLATFORM

Azure
- IaaS
- PaaS
- Compute, Application and Data Services

BUSINESS APPS

- Configure Your Own SaaS Applications
- Manage Relational Data
- Build Custom Applications for your business

MEET YOUR COMPLIANCE REQUIREMENTS

- Compliance is one of the biggest challenges many organizations face
- Office 365 uses the HIPAA Business Associate Agreement to establish responsible parties for implementation of physical, technical, and administrative safeguards.
- Meets the breach notification requirements of HITECH, ISO 27001, Federal Information Security Management Act (FISMA), EU Safe Harbor, EU ModelClauses, and the Data Processing Agreement
- Global Data Protection Agreement (GDPR) compliance expected May 2018
CYBERSECURITY TODAY IS POWERED BY:

✓ Provide your organization with flexible, familiar apps and services that enhance employee productivity and allow access from virtually anywhere

✓ Identity-driven tools help you stay secure and productive on your favorite apps and devices

✓ Microsoft managed security built to secure O365 and Azure data and content

Bundled Together = Microsoft 365

SECURITY AND COMPLIANCE TOOLS

- Each Office 365 “Tenant” has a Security and Compliance Center
- Set up business rules to prevent data loss, govern data/content, and monitor threats
DON'T FORGET YOUR DEVICES

- Need to be Secured
- Enterprise Mobility + Security locks down content and devices
- Windows 10 enhances device security

Poll: Does your firm have a Cloud Strategy?
Making Your Cloud Strategy Actually Work!

STEP 1: UNDERSTAND YOUR CONTENT

Do You have an existing Cloud Strategy?

What steps has your firm already taken?

• Most firms have adopted some sort of cloud technology
• Business Apps (Office 365, Google for Work, etc.)
• Email perhaps one of the most common cloud technologies

So what happens without a good strategy?

• Uneven adoption
• Unable to achieve tactical objectives
• You will complicate your IT operations
STEP 2: UNDERSTAND YOUR BUSINESS DRIVERS

To be successful, you need to know:

- The compelling business reasons/drivers to move to the Cloud
- How stakeholders align with those drivers
- How your existing strategy aligns with your 2016 adoption plans

The three most common drivers

- Improve agility of business
- Transform IT Ops (not necessarily cost-driven)
- Reduce Costs (IT or business costs)

COMMON CLOUD BUSINESS DRIVERS

- Increase Business Agility
- Transform IT Operations
- Reduce IT Footprint
- Reduce time-to-develop
- Improve Agility
- Control HW/SW Sprawl
- Involve business in development
- Increase IT ROI
- Reduce IT Costs
STEP 3: KNOW THE IMPACTS OF CLOUD ADOPTION

Initial Move to the Cloud

- Most Impacts are Non-Technical
  - People (including Organizational)
  - Business Processes
  - Governance Policies
  - Budgets
- Some are Technical
  - IT Architecture (Hybrid Environment)
- These Ultimately Impact ROI
- Must be Carefully Managed

Aligning with an Existing Cloud Strategy

IMPACTS ON PEOPLE AND ORGANIZATIONS

<table>
<thead>
<tr>
<th>People</th>
<th>Organizational/Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Developer Skill Sets will Change</td>
<td>IT Organization will change</td>
</tr>
<tr>
<td>• Developers will Need Cloud Programming Skills</td>
<td></td>
</tr>
<tr>
<td>• Integration Skills for Hybrid Environments</td>
<td></td>
</tr>
<tr>
<td>• Understand Cloud Security</td>
<td></td>
</tr>
<tr>
<td>• Mobile</td>
<td></td>
</tr>
<tr>
<td>Infrastructure Support Staff</td>
<td>Shift from on-premise service provider to managing a hybrid environment</td>
</tr>
<tr>
<td>• Must be able to Manage Hybrid Environments</td>
<td>• Composite app provider</td>
</tr>
<tr>
<td>• Requirement for Infrastructure Support Skills will Decrease Over Time</td>
<td>• Manage on-prem and cloud vendor relationships</td>
</tr>
<tr>
<td></td>
<td>Governance and Policy Changes</td>
</tr>
<tr>
<td></td>
<td>• Need policies and governance for the hybrid environment</td>
</tr>
</tbody>
</table>
IMPACTS ON BUSINESS PROCESSES

Processes may be Eliminated, Changed, or Added
• Dependent on Types of Services Moved to the Cloud

Identify and Analyze how Core Processes are Affected

Keep In Mind
• Changes to Processes will Normally Incur Costs
• Will Impact on People (Feedback Loop)

IMPACTS ON BUDGETS

Moving to the Cloud Shifts Costs from Capital Costs to Operational Costs (Capex to Opex)
• This is usually a concern for larger firms

Don’t Forget to Assess Your License Commitments
• Time Your Move to the Cloud with HW/SW License Renewal Cycle to Extent Possible

Understand How Cloud Charges are Incurred
IT ENVIRONMENT IMPACTS

- Hybrid Environments Becoming the Norm
- Imposes Changes to:
  - Administration
  - Governance/Policies
  - Developers
- All Need to be Factored into Costs and Budget Planning

UNDERSTANDING ARCHITECTURAL CHANGES

- As you adopt the Cloud...you will probably build a hybrid environment
- "Most Enterprises are not Migrating Apps to the Cloud – They are Evolving Them"
  - James Staten, VP Principal Analyst at Forrester
  - Why and How Firms are Adopting Cloud Platforms (February 18 2015)
  - Currently Chief Strategist: Cloud + Enterprise Division
- Cloud Vendors (often different ones) will have to integrate with your environment
**STEP 4: CREATE OR ADJUST YOUR CLOUD STRATEGY**

- Increase Business Agility
- Transform IT Operations
- Reduce IT Footprint
- Reduce time-to-develop
- Improve Agility
- Control HW/SW Sprawl
- Involve business in development
- Increase IT ROI
- Reduce IT Costs

**Don’t Have One?**
- Get One: Template coming soon!

**Clearly identify goals of the Overall Strategy**
- Simplify IT?
- Reduce Costs?

**Adjust the strategy based on actual experiences**

**STEP 5: CREATE YOUR ROADMAP**

- Increase Business Agility
- Transform IT Operations
- Reduce IT Footprint
- Reduce time-to-develop
- Improve Agility
- Control HW/SW Sprawl
- Involve business in development
- Increase IT ROI
- Reduce IT Costs

**Select cloud services that align with your strategy**

**Create a practical 2018 Roadmap**
- Pick low-risk, high-payoff Cloud services
- Gain experience with those services

**Understand the impacts these services will have**
1. Move Dev/Test to the Cloud
   • Get on the Dev/Ops bandwagon
   • Azure is a great Platform to do this
     • Infrastructure-as-a-Service (IaaS)
     • Platform-as-a-Service (PaaS)

2. Use Office 365 for Collaboration/Social
   • O365 a great way to start with the cloud
   • Bundled SaaS tools
Understanding the Value of Cloud Business Planning

WHY PLANNING MATTERS

- Responding *Ad Hoc* to Changes and Impacts of Cloud Adoption Places You Behind the Curve
  - Scrambling to find the Developers, Managers, and Other Staff with the Skills You Need
  - Creating Non-standard Governance, Development, and Other Administrative Procedures

- Decreases Efficiency
- Introduces Opportunity for Security Issues Downstream
- Delays ROI and Business Value
2018 PLANNING PROCESS

Inputs

• Stakeholder expectations
• Business drivers and goals
• Identify and quantify impacts to:
  • People
  • Organizations
  • Governance/admin policies
  • IT environment
• Understand costs
• ROI for each investment

Assets

• Statement of business objectives
• Future IT vision (Cloud Strategy) roadmap
• Each subsequent project/migration requires validation against these strategic assets

ANTICIPATE THE COMING CHANGES

• Identify and Quantify Changes and Impacts
• Incorporate into Your ROI Projections
• Get the Right People to Deal with Hybrid Environments
• Benefits
  • Better Cost Control
  • Better Planning
  • Realistic ROI Projections
  • Greatly Improved Business Value
Understanding your third party network and risks
- AICPA SOC for Cybersecurity

THE NEW “SOC” – APRIL 2017

SOC - SERVICE ORGANIZATION CONTROLS

SOC - SYSTEM AND ORGANIZATION CONTROLS

SOC FOR SERVICE ORGANIZATIONS
- SOC 1® - ICFR
- SOC 2® - TRUST SERVICES CRITERIA
  - SOC 2® HITRUST
  - SOC 2® CSA STAR Attestation
- SOC 3® - GENERAL USE REPORT

SOC FOR CYBERSECURITY

SOC FOR VENDOR SUPPLY CHAINS UNDER DEVELOPMENT
WHO’S INTERESTED IN YOUR CYBER PRACTICES?

Information regarding the effectiveness of an Entity’s Cybersecurity practice is needed by:

- Those charged with governance – Board of Directors
- Investors
- Lenders
- Customers
- Regulators
- Vendors & Business Partners
Implementing Best Practices

- What you can do internally
### 25 MOST POPULAR PASSWORDS FROM 2017

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>(unchanged from 2016 list)</td>
</tr>
<tr>
<td>2</td>
<td>password</td>
<td>(unchanged)</td>
</tr>
<tr>
<td>3</td>
<td>12345678</td>
<td>(up one place)</td>
</tr>
<tr>
<td>4</td>
<td>qwerty</td>
<td>(up two places)</td>
</tr>
<tr>
<td>5</td>
<td>12345678</td>
<td>(down two places)</td>
</tr>
<tr>
<td>6</td>
<td>123456789</td>
<td>(new entry)</td>
</tr>
<tr>
<td>7</td>
<td>letmein</td>
<td>(new entry)</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>(unchanged)</td>
</tr>
<tr>
<td>9</td>
<td>football</td>
<td>(down four places)</td>
</tr>
<tr>
<td>10</td>
<td>loveyou</td>
<td>(new entry)</td>
</tr>
<tr>
<td>11</td>
<td>admin</td>
<td>(up four places)</td>
</tr>
<tr>
<td>12</td>
<td>welcome</td>
<td>(unchanged)</td>
</tr>
<tr>
<td>13</td>
<td>monkey</td>
<td>(new entry)</td>
</tr>
<tr>
<td>14</td>
<td>login</td>
<td>(down three places)</td>
</tr>
<tr>
<td>15</td>
<td>abc123</td>
<td>(down one place)</td>
</tr>
<tr>
<td>16</td>
<td>starwars</td>
<td>(new entry)</td>
</tr>
<tr>
<td>17</td>
<td>123123</td>
<td>(new entry)</td>
</tr>
<tr>
<td>18</td>
<td>dragon</td>
<td>(up one place)</td>
</tr>
<tr>
<td>19</td>
<td>pasaw0rd</td>
<td>(down one place)</td>
</tr>
<tr>
<td>20</td>
<td>master</td>
<td>(up one place)</td>
</tr>
<tr>
<td>21</td>
<td>hello</td>
<td>(new entry)</td>
</tr>
<tr>
<td>22</td>
<td>freedom</td>
<td>(new entry)</td>
</tr>
<tr>
<td>23</td>
<td>whatever</td>
<td>(new entry)</td>
</tr>
<tr>
<td>24</td>
<td>qazwxs</td>
<td>(new entry)</td>
</tr>
<tr>
<td>25</td>
<td>trustno1</td>
<td>(new entry)</td>
</tr>
</tbody>
</table>

Raise your hand if you use one of these...

### WEAK PASSWORDS - THE MOST COMMON THREAT

- Passwords are the most common security mechanism used in technology
- They are also the most common item attacked
- Ensuring that you abide by password best-practices will help protect you and your organization

© Digital 4NX Group, Ltd. 2017. All rights reserved.
WEAK PASSWORDS - THE MOST COMMON THREAT

PASSWORDS ARE LIKE UNDERPANTS

Change them often, keep them private and never share them with anyone.

SPEED TO CRACK PASSWORDS

Here is how long it takes to crack passwords of various complexities:

- 6 Alpha characters (e.g. monkey) – 1 second
- 6 Alpha-Numeric characters (e.g. abc123) – 1 second
- 8 Alpha characters (e.g. password) - 1 minute
- 8 Alpha-Numeric characters (e.g. trustno1) - 11 minutes
- 8 Alpha-Numeric + Special characters (e.g. tr1cky!!) - 3 hours
- 8 Upper & Lowercase, Numbers + Special (e.g. Tr1cky!!) - 3 days
- 10 Upper & Lowercase, Numbers + Special (e.g. I’mTr1cky!) - 58 years

For example, My son’s birthday is 12 December, 2004 could become Mi$un’s Brthd8iz 12124, which would make a good passphrase.

*Based on the processing power of a desktop PC. These time can be sped up if a hacker has more powerful servers or resources. Your password can also be easier to crack if you use dictionary words or a commonly used password.
PASSWORDS – BEST PRACTICES

- Do not use names, dates, or dictionary words.
- Use long passphrases which are easy to remember.
- Length matters. Passwords should be at least 8 characters and contain numbers, capital letters and symbols.
- Change passwords on at least a quarterly basis.
- Always use two-factor authentication if offered by the provider.
- Never use the same password in different accounts.

HOW TO STORE

Rules

- Don’t write your password down on a sticky-note attached to your screen
- Don’t keep your passwords written in a text file on your computer
- Don’t write them down in plaintext anywhere!
- Instead, Use secure pass-phrases that you can remember, or
- Use an encrypted password storage program, like KeePass or LastPass
The most important account to protect is your **email account**. If an attacker gains access to your email account, they can reset access to most other accounts *(Unless you are using two-factor authentication of course!)*

Use a **STRONG** and **UNIQUE** password for your email account. Protect this account above all else; it is the primary target of hackers.

---

**MULTI-FACTOR / TWO-FACTOR AUTHENTICATION**

- Authentication is either:
  - Something you know *(like a password or PIN)*
  - Something you have *(like your cellphone or ATM card)*
  - Something you are *(like your fingerprint)*

- Passwords are the common form used
- Adding a second factor greatly increases security
- A common option being used now is to send a code via text to your cell phone *(something you have)* and asking for that in addition to your password *(something you know)*

- Turn on 2-Factor Authentication for added security, especially with email accounts, bank accounts, and other sensitive accounts
Free Tools:
- BitLocker
- GNU Privacy Guard
- VeraCrypt
- Disk Utility (Mac OS only)
- AxCrypt
- CipherShed
- Add Description
- Many More

Encrypt a hard drive or USB flash:

Be cautious and wary:
- Many attacks rely on tricking the user and playing on their lack of suspicion.
- Don’t be the low-lying fruit; attacks are often aimed at the easiest prey and criminals will move along to another target if they encounter defenses.
- When in doubt, play it safe. Ask someone if you are not sure.

All it takes is one mistake. Be naturally cautious and wary.
KEY TAKEAWAYS

- It is not a question of if but when
- Know and test for your weaknesses
- Know where is your data and who has access
- Invest now with breach cost reduction tips
- Thoroughly test your third party network regularly
- Embrace the cloud – don’t be overly skeptical

THANK YOU / QUESTIONS ??

Rob Kleeger
Founder and Managing Director
Digital Forensic Investigations | Incident Response Data Breaches | Cyber Security
rkleeger@Digital4nxGroup.com
973.699.0167

Joe Riccie, Partner
Market Leader
Cyber & Information Security Services
jriccie@withum.com
908.303.2354
Your opinion matters!

Please take a moment now to complete the evaluation.

Thank You!