Get into the Cloud
Safely and Securely

bryleysystems®
MANAGED IT SERVICES
Manage • Optimize • Secure – Since 1987™

Bryley Systems Inc.

Gavin H. Livingstone

- President, Bryley Systems Inc.
- Over 30 years in computer support
- MBA from Boston College, Novell CNE, Microsoft MCSE

Bryley Systems is a full-service partner, fulfilling the information-technology needs of our clients throughout central New England since 1987.

Visit www.Bryley.com for more information.

Synopsis

Cloud Services and your data; learn how to select from Cloud options while protecting yourself from internal and external threats:

- How to compare popular Cloud Services
- Preventative measures to secure your Cloud Services
- How to ensure the integrity of your valuable data, whether inside your office or out in the Cloud

Agenda

I. Comparing Cloud Services
   - A. Going to the Cloud
   - B. Cloud Computing Service Models
   - C. Public, Private, and Hybrid Clouds
   - D. Common SaaS Cloud Services
   - E. Selection Process
   - F. Securing Cloud Services

II. Preventative Measures
   - A. Computer and Internet/Cloud-Use policy
   - B. Security Policy
   - C. User Education
   - D. Technologies

III. Data Integrity
   - A. Backup
   - B. Disaster Recovery

I. Comparing Cloud Services

A. Going to the Cloud
B. Cloud Computing Service Models
C. Public, Private, and Hybrid Clouds
D. Common SaaS Cloud Services
E. Selection Process
F. Securing Cloud Services

Going to the Cloud

- Benefits:
  - Eliminate up-front capital expenditure
  - Reduce operating costs
  - Access from anywhere
- Considerations:
  - Ensure sufficient bandwidth, both up and down
  - Consider Internet fail-over to ensure availability
  - Most start small and expand gradually

Cloud Computing Service Models

- Software as a Service (SaaS):
  - On-demand software; software and data hosted in Cloud
  - Common applications: CRM, ERP, HRM, accounting, etc.
  - Web-based interface with subscription fee per user
- Platform as a Service (PaaS):
  - Basic components (virtual machines, software) to build on
  - Consumer creates the software
- Infrastructure as a Service (IaaS):
  - Raw infrastructure (computing hardware, storage, etc.)
  - Consumer deploys servers and creates entire environment

Public, Private, and Hybrid Clouds

- Public Cloud – Cloud-based resources available to anyone
- Private Cloud – Dedicated Cloud environment:
  - Hosted services to a limited number of people
  - Usually exclusive Virtual Machine(s)
  - Protected behind a firewall
  - Often accessed via VPN
- Hybrid – Interfaced Cloud Services:
  - Combination of two or more Clouds (Private, Public)
  - Often refers to mix of on-premise plus Cloud-based resources (two layer)

Go to http://www.Bryley.com/Hosted-Cloud-Server/ for details on Bryley's Hosted Cloud Server, our private-cloud service.

Common SaaS Cloud Services

- Prevention
- Productivity Suites
- Storage
- Backup and Recovery

Visit http://www.Bryley.com/Solutions/Cloud-Computing/ to see our Cloud Services.

SaaS – Prevention

- Most organizations start with Prevention
- Primary options within Prevention:
  - Email protection – Controls spam plus offers email encryption and archiving
  - End-point security – Secure end-user computers against external attacks
  - Web filtering – Prevent/log unauthorized access to undesired websites
- Popular email-protection options include:
  - McAfee Email Protection – Continuity & Outbound at $27/user per year
  - Microsoft Exchange Online Protection – Exchange only at $12/user per year
  - ProofPoint Essentials Business – Outbound & spooling at $26.40/user per year
- Endpoint security from McAfee, Symantec, AVG, Kaspersky
- Web filtering from McAfee, Axway (Tumbleweed), WebSense
- See http://www.Bryley.com/McAfee-SaaS/ for McAfee options
- We also offer secure transfer: http://www.Bryley.com/Leapfile/

SaaS – Productivity Suites

- Suite of word processing, spreadsheet, slideshow, calendar, email, storage, and other applications
- Google Apps for Business:
  - $50/user per year
  - One size fits all across multiple devices
- Microsoft Office 365:
  - Options start at $48/year, but common at $96/year and up
  - Greater functionality with familiar interface
  - Primarily Windows-based devices
  - Visit http://www.Bryley.com/Office365/

SaaS – Storage

- Desired features (often found only in paid versions):
  - Plans start at $5/user per month; price increases with features & space
  - File synchronization across multiple devices
  - Security with rotating encryption keys
  - Access control and auditing
  - AD/LDAP integration
- Popular options include:
  - Box.net – 10Gb free; highly secure and comprehensive (integration, access control, etc.) offering. Also, NetSkope second-highest rating.
  - Dropbox – 2Gb free; over 200M subscribers. Easiest and most fun to use, but a bit more expensive than comparable offerings.
  - Google Drive – 15Gb free; no frills, but very reliable at reasonable cost.
  - Microsoft OneDrive – 7Gb free; offers the most for the least. Includes unique “Fetch” (from a PC) feature and integrates within MS Office.

SaaS – Backup and Recovery

- Desired features:
  - Automatically copy image or folders and files to Cloud periodically
  - Secure via encryption and somewhat resistant to attack
  - Held separately, unchanged, for recovery purposes
- Popular options include:
  - Carbonite – Extremely popular; automated, encrypted, and easy to use. Starts at $59.99/device per year; business plans start at $299.99/year.
  - Mozy – Well-known with both home and business versions. Home starts at $5.99/device per month; business plans start at $26.98/month.
  - SOS Online Backup – Includes monitoring, password encryption, and phone support. Pricing at $9.99/user per month; unlimited users and devices at $99.99 per month.
- Bryley BU/DR at http://www.Bryley.com/Backup-Data-Recovery

Selection Process

- Primary concerns:
  - Privacy – Based on type of encryption:
    - How are they protecting your data?
    - What tools are used to protect data from third-party access?
  - Resiliency – Measure dependability of the vendor's service via SLA:
    - How much downtime? Conversely, how much uptime (five 9s) or availability?
    - What protocols in-place during downtime? Any remuneration if SLA not met?
  - Customization – What to move to the Cloud and when:
    - Can vendor support a two-layered approach (on-premise plus Cloud)?
    - Can the vendor scale to your needs?
  - Control – More control can reduce Total Cost of Ownership:
    - What can I configure and manage myself through policies via the admin interface?
    - What is no longer available to me?
  - Support – Essential for satisfaction, security, and when things go wrong

Details at http://www.eweek.com/c/a/Cloud-Computing/How-to-Assess-CloudBased-EMail-Security-Vendors/.

Selection Process (continued)

- Key issues:
  - Administration – Easy setup and enforcement
  - Effectiveness – Works reliably and consistently
  - End-user interface – Intuitive, secure, and friendly
  - Granularity – Allows multi-level policies and permissions

Securing Cloud Services

Top 9 threats to Cloud Services in 2013:

1. Data breach – Usually externally, but internal assistance
2. Data loss – Disaster, malware, or lost encryption key
3. Hijacking – Account or service traffic
4. Insecure interfaces and APIs – Awareness
5. Denial of Service (DoS) – Slows performance; increase cost
6. Malicious insiders – Unnecessary access, bad passwords
7. Cloud abuse – Using Cloud computing malevolently
8. Insufficient due diligence – Understand the risks
9. Shared technologies – Shared infrastructure and platform

Visit http://www.Infoworld.com/t/Cloud-Security/9-top-threats-cloud-computing-security-213428.

Securing Cloud Services (cont.)

- Cloud Services provider:
  - Proper provisioning and deployment of Virtual Machines
  - Multi-level security at all points of entry
  - Secure access
- Your habits should include:
  - Proper policies and Internet/Cloud-use procedures
  - Remote backup separate from other services
  - Two-factor authentication where available
  - Preventative measures
  - Disaster Recovery plan

II. Preventative Measures

A. Computer and Internet/Cloud-Use Policy

B. Security Policy

C. User Education

D. Technologies

Preventative – Computer and Internet/Cloud-Use Policy

- Defines how employees use computer and Internet (Cloud) while reducing organization's liability
- Should be as formal as other policy documents
- Objectives:
  - Reduce or eliminate unproductive use (personal shopping, entertainment, etc.)
  - Prohibit illegal use (downloading copyrighted materials, gambling, pornography, etc.)
  - Limit legal liability (sexual harassment, illegal activities)

Preventative – Computer and Internet/Cloud-Use Policy (continued)

- Include within Employee Manual
- Require separate sign-off
- Some suggestions:
  - Use only company-provided Cloud Services
  - Use only company-approved software
  - Do not share accounts and passwords
  - Restrict to business-use only

Preventative – Security Policy

- Complements Computer & Internet/Cloud-Use policy
- Defines, from a technology standpoint, what is allowed and not allowed in the Cloud and on the local network
- Defines the process for making changes, including who authorizes these changes
- Written Security Information Program (WISP)
- Include within Employee Manual
- Require separate sign-off

Preventative – User Education

- Essential to the health of your Cloud Services and your on-premise computer network
- Provide ongoing training:
  - Safe browsing
  - Avoiding phishing and scams
  - Proper password use and storage
  - Do not download viruses and spyware
- Some organizations phish internal users; once hooked, IT provides immediate feedback

Preventative – Technologies

- Operating System
- Firewall
- VPN
- Layering

Technologies – Operating System

- Interface Active Directory or LDAP to Cloud Services
- All users must have own username and password
- Require password complexity with periodic changes
- Use file and directory security to restrict access
- Enable auditing and/or encryption on sensitive data
- Limit administrative access: Administrators use a non-privileged account for day-to-day activities

Technologies – Firewall

- Controls network traffic between its interfaces (typically between local network and Cloud)
- Default rules block most inbound traffic while allowing outbound traffic
- Stateful packet inspection is a required feature
- Universal Threat Management on some appliances
- Automatic circuit fail-over on higher-end models
- See http://www.Bryley.com/Secure-Network/

Technologies – VPN

- Encrypted connection over the Internet
- Primary site requires a VPN-hardware device
- Remote connection can be via a hardware device, login (SSL), or a software client (IPSec)
- Required for Bryley's Hosted Cloud Server; it provides secure connection for Private Cloud

Technologies – Layering

- Create multiple, redundant, levels of protection
- Provide multi-vendor solutions at key areas
- Like home security; the more layers (door locks plus deadbolt, window locks, open/closed sensors, motion sensors, security cameras, etc.) the better.
- Bryley layering for 201 CMR 17.00 compliance:
  - Comprehensive Support Program
  - Secure Network
  - Multi-Point Security Hardening Service
  - Visit http://www.Bryley.com/Solutions/Network-Security/

III. Data Integrity

A. Backup

B. Disaster Recovery

Integrity – Backup

- Store all data at on-premise servers or in the Cloud (rather than on workstations)
- Deploy data-backup plan:
  - Who manages the process
  - Define where and how backups are stored offsite
  - What gets backed-up (server image, folders, files)
  - How often do backups run (continuous, periodically)
- Get our free 2014 Data-Backup Guidelines at http://www.Bryley.com/Bryley-Data-Backup-Guidelines-2014/

Integrity – Disaster Recovery

- Build/ensure appropriate levels of redundancy in all business-critical systems:
  - Phone system
  - Cloud Services
  - Computer network
- Create and distribute a contingency plan:
  - What offsite resources are available where
  - Who does what, where, and when
- Test often; especially restoration of backups

Get into the Cloud
Safely and Securely

bryleysystems®
MANAGED IT SERVICES
Manage • Optimize • Secure – Since 1987™

Bryley Systems Inc.

Gavin H. Livingstone

- President, Bryley Systems Inc.
- Over 30 years in computer support
- MBA from Boston College, Novell CNE, Microsoft MCSE

Bryley Systems is a full-service partner, fulfilling the information-technology needs of our clients throughout central New England since 1987.

Visit www.Bryley.com for more information.

Synopsis

Cloud Services and your data; learn how to select from Cloud options while protecting yourself from internal and external threats:

- How to compare popular Cloud Services
- Preventative measures to secure your Cloud Services
- How to ensure the integrity of your valuable data, whether inside your office or out in the Cloud

Agenda

I. Comparing Cloud Services
   - A. Going to the Cloud
   - B. Cloud Computing Service Models
   - C. Public, Private, and Hybrid Clouds
   - D. Common SaaS Cloud Services
   - E. Selection Process
   - F. Securing Cloud Services

II. Preventative Measures
   - A. Computer and Internet/Cloud-Use policy
   - B. Security Policy
   - C. User Education
   - D. Technologies

III. Data Integrity
   - A. Backup
   - B. Disaster Recovery

I. Comparing Cloud Services

A. Going to the Cloud
B. Cloud Computing Service Models
C. Public, Private, and Hybrid Clouds
D. Common SaaS Cloud Services
E. Selection Process
F. Securing Cloud Services

Going to the Cloud

- Benefits:
  - Eliminate up-front capital expenditure
  - Reduce operating costs
  - Access from anywhere
- Considerations:
  - Ensure sufficient bandwidth, both up and down
  - Consider Internet fail-over to ensure availability
  - Most start small and expand gradually

Cloud Computing Service Models

- Software as a Service (SaaS):
  - On-demand software; software and data hosted in Cloud
  - Common applications: CRM, ERP, HRM, accounting, etc.
  - Web-based interface with subscription fee per user
- Platform as a Service (PaaS):
  - Basic components (virtual machines, software) to build on
  - Consumer creates the software
- Infrastructure as a Service (IaaS):
  - Raw infrastructure (computing hardware, storage, etc.)
  - Consumer deploys servers and creates entire environment

Public, Private, and Hybrid Clouds

- Public Cloud – Cloud-based resources available to anyone
- Private Cloud – Dedicated Cloud environment:
  - Hosted services to a limited number of people
  - Usually exclusive Virtual Machine(s)
  - Protected behind a firewall
  - Often accessed via VPN
- Hybrid – Interfaced Cloud Services:
  - Combination of two or more Clouds (Private, Public)
  - Often refers to mix of on-premise plus Cloud-based resources (two layer)

Go to http://www.Bryley.com/Hosted-Cloud-Server/ for details on Bryley's Hosted Cloud Server, our private-cloud service.

Common SaaS Cloud Services

- Prevention
- Productivity Suites
- Storage
- Backup and Recovery

Visit http://www.Bryley.com/Solutions/Cloud-Computing/ to see our Cloud Services.

SaaS – Prevention

- Most organizations start with Prevention
- Primary options within Prevention:
  - Email protection – Controls spam plus offers email encryption and archiving
  - End-point security – Secure end-user computers against external attacks
  - Web filtering – Prevent/log unauthorized access to undesired websites
- Popular email-protection options include:
  - McAfee Email Protection – Continuity & Outbound at $27/user per year
  - Microsoft Exchange Online Protection – Exchange only at $12/user per year
  - ProofPoint Essentials Business – Outbound & spooling at $26.40/user per year
- Endpoint security from McAfee, Symantec, AVG, Kaspersky
- Web filtering from McAfee, Axway (Tumbleweed), WebSense
- See http://www.Bryley.com/McAfee-SaaS/ for McAfee options
- We also offer secure transfer: http://www.Bryley.com/Leapfile/

SaaS – Productivity Suites

- Suite of word processing, spreadsheet, slideshow, calendar, email, storage, and other applications
- Google Apps for Business:
  - $50/user per year
  - One size fits all across multiple devices
- Microsoft Office 365:
  - Options start at $48/year, but common at $96/year and up
  - Greater functionality with familiar interface
  - Primarily Windows-based devices
  - Visit http://www.Bryley.com/Office365/

SaaS – Storage

- Desired features (often found only in paid versions):
  - Plans start at $5/user per month; price increases with features & space
  - File synchronization across multiple devices
  - Security with rotating encryption keys
  - Access control and auditing
  - AD/LDAP integration
- Popular options include:
  - Box.net – 10Gb free; highly secure and comprehensive (integration, access control, etc.) offering. Also, NetSkope second-highest rating.
  - Dropbox – 2Gb free; over 200M subscribers. Easiest and most fun to use, but a bit more expensive than comparable offerings.
  - Google Drive – 15Gb free; no frills, but very reliable at reasonable cost.
  - Microsoft OneDrive – 7Gb free; offers the most for the least. Includes unique “Fetch” (from a PC) feature and integrates within MS Office.

SaaS – Backup and Recovery

- Desired features:
  - Automatically copy image or folders and files to Cloud periodically
  - Secure via encryption and somewhat resistant to attack
  - Held separately, unchanged, for recovery purposes
- Popular options include:
  - Carbonite – Extremely popular; automated, encrypted, and easy to use. Starts at $59.99/device per year; business plans start at $299.99/year.
  - Mozy – Well-known with both home and business versions. Home starts at $5.99/device per month; business plans start at $26.98/month.
  - SOS Online Backup – Includes monitoring, password encryption, and phone support. Pricing at $9.99/user per month; unlimited users and devices at $99.99 per month.
- Bryley BU/DR at http://www.Bryley.com/Backup-Data-Recovery

Selection Process

- Primary concerns:
  - Privacy – Based on type of encryption:
    - How are they protecting your data?
    - What tools are used to protect data from third-party access?
  - Resiliency – Measure dependability of the vendor's service via SLA:
    - How much downtime? Conversely, how much uptime (five 9s) or availability?
    - What protocols in-place during downtime? Any remuneration if SLA not met?
  - Customization – What to move to the Cloud and when:
    - Can vendor support a two-layered approach (on-premise plus Cloud)?
    - Can the vendor scale to your needs?
  - Control – More control can reduce Total Cost of Ownership:
    - What can I configure and manage myself through policies via the admin interface?
    - What is no longer available to me?
  - Support – Essential for satisfaction, security, and when things go wrong

Details at http://www.eweek.com/c/a/Cloud-Computing/How-to-Assess-CloudBased-EMail-Security-Vendors/.

Selection Process (continued)

- Key issues:
  - Administration – Easy setup and enforcement
  - Effectiveness – Works reliably and consistently
  - End-user interface – Intuitive, secure, and friendly
  - Granularity – Allows multi-level policies and permissions

Securing Cloud Services

Top 9 threats to Cloud Services in 2013:

1. Data breach – Usually externally, but internal assistance
2. Data loss – Disaster, malware, or lost encryption key
3. Hijacking – Account or service traffic
4. Insecure interfaces and APIs – Awareness
5. Denial of Service (DoS) – Slows performance; increase cost
6. Malicious insiders – Unnecessary access, bad passwords
7. Cloud abuse – Using Cloud computing malevolently
8. Insufficient due diligence – Understand the risks
9. Shared technologies – Shared infrastructure and platform

Visit http://www.Infoworld.com/t/Cloud-Security/9-top-threats-cloud-computing-security-213428.

Securing Cloud Services (cont.)

- Cloud Services provider:
  - Proper provisioning and deployment of Virtual Machines
  - Multi-level security at all points of entry
  - Secure access
- Your habits should include:
  - Proper policies and Internet/Cloud-use procedures
  - Remote backup separate from other services
  - Two-factor authentication where available
  - Preventative measures
  - Disaster Recovery plan

II. Preventative Measures

A. Computer and Internet/Cloud-Use Policy

B. Security Policy

C. User Education

D. Technologies

Preventative – Computer and Internet/Cloud-Use Policy

- Defines how employees use computer and Internet (Cloud) while reducing organization's liability
- Should be as formal as other policy documents
- Objectives:
  - Reduce or eliminate unproductive use (personal shopping, entertainment, etc.)
  - Prohibit illegal use (downloading copyrighted materials, gambling, pornography, etc.)
  - Limit legal liability (sexual harassment, illegal activities)

Preventative – Computer and Internet/Cloud-Use Policy (continued)

- Include within Employee Manual
- Require separate sign-off
- Some suggestions:
  - Use only company-provided Cloud Services
  - Use only company-approved software
  - Do not share accounts and passwords
  - Restrict to business-use only

Preventative – Security Policy

- Complements Computer & Internet/Cloud-Use policy
- Defines, from a technology standpoint, what is allowed and not allowed in the Cloud and on the local network
- Defines the process for making changes, including who authorizes these changes
- Written Security Information Program (WISP)
- Include within Employee Manual
- Require separate sign-off

Preventative – User Education

- Essential to the health of your Cloud Services and your on-premise computer network
- Provide ongoing training:
  - Safe browsing
  - Avoiding phishing and scams
  - Proper password use and storage
  - Do not download viruses and spyware
- Some organizations phish internal users; once hooked, IT provides immediate feedback

Preventative – Technologies

- Operating System
- Firewall
- VPN
- Layering

Technologies – Operating System

- Interface Active Directory or LDAP to Cloud Services
- All users must have own username and password
- Require password complexity with periodic changes
- Use file and directory security to restrict access
- Enable auditing and/or encryption on sensitive data
- Limit administrative access: Administrators use a non-privileged account for day-to-day activities

Technologies – Firewall

- Controls network traffic between its interfaces (typically between local network and Cloud)
- Default rules block most inbound traffic while allowing outbound traffic
- Stateful packet inspection is a required feature
- Universal Threat Management on some appliances
- Automatic circuit fail-over on higher-end models
- See http://www.Bryley.com/Secure-Network/

Technologies – VPN

- Encrypted connection over the Internet
- Primary site requires a VPN-hardware device
- Remote connection can be via a hardware device, login (SSL), or a software client (IPSec)
- Required for Bryley's Hosted Cloud Server; it provides secure connection for Private Cloud

Technologies – Layering

- Create multiple, redundant, levels of protection
- Provide multi-vendor solutions at key areas
- Like home security; the more layers (door locks plus deadbolt, window locks, open/closed sensors, motion sensors, security cameras, etc.) the better.
- Bryley layering for 201 CMR 17.00 compliance:
  - Comprehensive Support Program
  - Secure Network
  - Multi-Point Security Hardening Service
  - Visit http://www.Bryley.com/Solutions/Network-Security/

III. Data Integrity

A. Backup

B. Disaster Recovery

Integrity – Backup

- Store all data at on-premise servers or in the Cloud (rather than on workstations)
- Deploy data-backup plan:
  - Who manages the process
  - Define where and how backups are stored offsite
  - What gets backed-up (server image, folders, files)
  - How often do backups run (continuous, periodically)
- Get our free 2014 Data-Backup Guidelines at http://www.Bryley.com/Bryley-Data-Backup-Guidelines-2014/

Integrity – Disaster Recovery

- Build/ensure appropriate levels of redundancy in all business-critical systems:
  - Phone system
  - Cloud Services
  - Computer network
- Create and distribute a contingency plan:
  - What offsite resources are available where
  - Who does what, where, and when
- Test often; especially restoration of backups

Get into the Cloud
Safely and Securely

bryleysystems®
MANAGED IT SERVICES
Manage • Optimize • Secure – Since 1987™

Bryley Systems Inc.

Gavin H. Livingstone

- President, Bryley Systems Inc.
- Over 30 years in computer support
- MBA from Boston College, Novell CNE, Microsoft MCSE

Bryley Systems is a full-service partner, fulfilling the information-technology needs of our clients throughout central New England since 1987.

Visit www.Bryley.com for more information.

Synopsis

Cloud Services and your data; learn how to select from Cloud options while protecting yourself from internal and external threats:

- How to compare popular Cloud Services
- Preventative measures to secure your Cloud Services
- How to ensure the integrity of your valuable data, whether inside your office or out in the Cloud

Agenda

I. Comparing Cloud Services
   - A. Going to the Cloud
   - B. Cloud Computing Service Models
   - C. Public, Private, and Hybrid Clouds
   - D. Common SaaS Cloud Services
   - E. Selection Process
   - F. Securing Cloud Services

II. Preventative Measures
   - A. Computer and Internet/Cloud-Use policy
   - B. Security Policy
   - C. User Education
   - D. Technologies

III. Data Integrity
   - A. Backup
   - B. Disaster Recovery

I. Comparing Cloud Services

A. Going to the Cloud
B. Cloud Computing Service Models
C. Public, Private, and Hybrid Clouds
D. Common SaaS Cloud Services
E. Selection Process
F. Securing Cloud Services

Going to the Cloud

- Benefits:
  - Eliminate up-front capital expenditure
  - Reduce operating costs
  - Access from anywhere
- Considerations:
  - Ensure sufficient bandwidth, both up and down
  - Consider Internet fail-over to ensure availability
  - Most start small and expand gradually

Cloud Computing Service Models

- Software as a Service (SaaS):
  - On-demand software; software and data hosted in Cloud
  - Common applications: CRM, ERP, HRM, accounting, etc.
  - Web-based interface with subscription fee per user
- Platform as a Service (PaaS):
  - Basic components (virtual machines, software) to build on
  - Consumer creates the software
- Infrastructure as a Service (IaaS):
  - Raw infrastructure (computing hardware, storage, etc.)
  - Consumer deploys servers and creates entire environment

Public, Private, and Hybrid Clouds

- Public Cloud – Cloud-based resources available to anyone
- Private Cloud – Dedicated Cloud environment:
  - Hosted services to a limited number of people
  - Usually exclusive Virtual Machine(s)
  - Protected behind a firewall
  - Often accessed via VPN
- Hybrid – Interfaced Cloud Services:
  - Combination of two or more Clouds (Private, Public)
  - Often refers to mix of on-premise plus Cloud-based resources (two layer)

Go to http://www.Bryley.com/Hosted-Cloud-Server/ for details on Bryley's Hosted Cloud Server, our private-cloud service.

Common SaaS Cloud Services

- Prevention
- Productivity Suites
- Storage
- Backup and Recovery

Visit http://www.Bryley.com/Solutions/Cloud-Computing/ to see our Cloud Services.

SaaS – Prevention

- Most organizations start with Prevention
- Primary options within Prevention:
  - Email protection – Controls spam plus offers email encryption and archiving
  - End-point security – Secure end-user computers against external attacks
  - Web filtering – Prevent/log unauthorized access to undesired websites
- Popular email-protection options include:
  - McAfee Email Protection – Continuity & Outbound at $27/user per year
  - Microsoft Exchange Online Protection – Exchange only at $12/user per year
  - ProofPoint Essentials Business – Outbound & spooling at $26.40/user per year
- Endpoint security from McAfee, Symantec, AVG, Kaspersky
- Web filtering from McAfee, Axway (Tumbleweed), WebSense
- See http://www.Bryley.com/McAfee-SaaS/ for McAfee options
- We also offer secure transfer: http://www.Bryley.com/Leapfile/

SaaS – Productivity Suites

- Suite of word processing, spreadsheet, slideshow, calendar, email, storage, and other applications
- Google Apps for Business:
  - $50/user per year
  - One size fits all across multiple devices
- Microsoft Office 365:
  - Options start at $48/year, but common at $96/year and up
  - Greater functionality with familiar interface
  - Primarily Windows-based devices
  - Visit http://www.Bryley.com/Office365/

SaaS – Storage

- Desired features (often found only in paid versions):
  - Plans start at $5/user per month; price increases with features & space
  - File synchronization across multiple devices
  - Security with rotating encryption keys
  - Access control and auditing
  - AD/LDAP integration
- Popular options include:
  - Box.net – 10Gb free; highly secure and comprehensive (integration, access control, etc.) offering. Also, NetSkope second-highest rating.
  - Dropbox – 2Gb free; over 200M subscribers. Easiest and most fun to use, but a bit more expensive than comparable offerings.
  - Google Drive – 15Gb free; no frills, but very reliable at reasonable cost.
  - Microsoft OneDrive – 7Gb free; offers the most for the least. Includes unique “Fetch” (from a PC) feature and integrates within MS Office.

SaaS – Backup and Recovery

- Desired features:
  - Automatically copy image or folders and files to Cloud periodically
  - Secure via encryption and somewhat resistant to attack
  - Held separately, unchanged, for recovery purposes
- Popular options include:
  - Carbonite – Extremely popular; automated, encrypted, and easy to use. Starts at $59.99/device per year; business plans start at $299.99/year.
  - Mozy – Well-known with both home and business versions. Home starts at $5.99/device per month; business plans start at $26.98/month.
  - SOS Online Backup – Includes monitoring, password encryption, and phone support. Pricing at $9.99/user per month; unlimited users and devices at $99.99 per month.
- Bryley BU/DR at http://www.Bryley.com/Backup-Data-Recovery

Selection Process

- Primary concerns:
  - Privacy – Based on type of encryption:
    - How are they protecting your data?
    - What tools are used to protect data from third-party access?
  - Resiliency – Measure dependability of the vendor's service via SLA:
    - How much downtime? Conversely, how much uptime (five 9s) or availability?
    - What protocols in-place during downtime? Any remuneration if SLA not met?
  - Customization – What to move to the Cloud and when:
    - Can vendor support a two-layered approach (on-premise plus Cloud)?
    - Can the vendor scale to your needs?
  - Control – More control can reduce Total Cost of Ownership:
    - What can I configure and manage myself through policies via the admin interface?
    - What is no longer available to me?
  - Support – Essential for satisfaction, security, and when things go wrong

Details at http://www.eweek.com/c/a/Cloud-Computing/How-to-Assess-CloudBased-EMail-Security-Vendors/.

Selection Process (continued)

- Key issues:
  - Administration – Easy setup and enforcement
  - Effectiveness – Works reliably and consistently
  - End-user interface – Intuitive, secure, and friendly
  - Granularity – Allows multi-level policies and permissions

Securing Cloud Services

Top 9 threats to Cloud Services in 2013:

1. Data breach – Usually externally, but internal assistance
2. Data loss – Disaster, malware, or lost encryption key
3. Hijacking – Account or service traffic
4. Insecure interfaces and APIs – Awareness
5. Denial of Service (DoS) – Slows performance; increase cost
6. Malicious insiders – Unnecessary access, bad passwords
7. Cloud abuse – Using Cloud computing malevolently
8. Insufficient due diligence – Understand the risks
9. Shared technologies – Shared infrastructure and platform

Visit http://www.Infoworld.com/t/Cloud-Security/9-top-threats-cloud-computing-security-213428.

Securing Cloud Services (cont.)

- Cloud Services provider:
  - Proper provisioning and deployment of Virtual Machines
  - Multi-level security at all points of entry
  - Secure access
- Your habits should include:
  - Proper policies and Internet/Cloud-use procedures
  - Remote backup separate from other services
  - Two-factor authentication where available
  - Preventative measures
  - Disaster Recovery plan

II. Preventative Measures

A. Computer and Internet/Cloud-Use Policy

B. Security Policy

C. User Education

D. Technologies

Preventative – Computer and Internet/Cloud-Use Policy

- Defines how employees use computer and Internet (Cloud) while reducing organization's liability
- Should be as formal as other policy documents
- Objectives:
  - Reduce or eliminate unproductive use (personal shopping, entertainment, etc.)
  - Prohibit illegal use (downloading copyrighted materials, gambling, pornography, etc.)
  - Limit legal liability (sexual harassment, illegal activities)

Preventative – Computer and Internet/Cloud-Use Policy (continued)

- Include within Employee Manual
- Require separate sign-off
- Some suggestions:
  - Use only company-provided Cloud Services
  - Use only company-approved software
  - Do not share accounts and passwords
  - Restrict to business-use only

Preventative – Security Policy

- Complements Computer & Internet/Cloud-Use policy
- Defines, from a technology standpoint, what is allowed and not allowed in the Cloud and on the local network
- Defines the process for making changes, including who authorizes these changes
- Written Security Information Program (WISP)
- Include within Employee Manual
- Require separate sign-off

Preventative – User Education

- Essential to the health of your Cloud Services and your on-premise computer network
- Provide ongoing training:
  - Safe browsing
  - Avoiding phishing and scams
  - Proper password use and storage
  - Do not download viruses and spyware
- Some organizations phish internal users; once hooked, IT provides immediate feedback

Preventative – Technologies

- Operating System
- Firewall
- VPN
- Layering

Technologies – Operating System

- Interface Active Directory or LDAP to Cloud Services
- All users must have own username and password
- Require password complexity with periodic changes
- Use file and directory security to restrict access
- Enable auditing and/or encryption on sensitive data
- Limit administrative access: Administrators use a non-privileged account for day-to-day activities

Technologies – Firewall

- Controls network traffic between its interfaces (typically between local network and Cloud)
- Default rules block most inbound traffic while allowing outbound traffic
- Stateful packet inspection is a required feature
- Universal Threat Management on some appliances
- Automatic circuit fail-over on higher-end models
- See http://www.Bryley.com/Secure-Network/

Technologies – VPN

- Encrypted connection over the Internet
- Primary site requires a VPN-hardware device
- Remote connection can be via a hardware device, login (SSL), or a software client (IPSec)
- Required for Bryley's Hosted Cloud Server; it provides secure connection for Private Cloud

Technologies – Layering

- Create multiple, redundant, levels of protection
- Provide multi-vendor solutions at key areas
- Like home security; the more layers (door locks plus deadbolt, window locks, open/closed sensors, motion sensors, security cameras, etc.) the better.
- Bryley layering for 201 CMR 17.00 compliance:
  - Comprehensive Support Program
  - Secure Network
  - Multi-Point Security Hardening Service
  - Visit http://www.Bryley.com/Solutions/Network-Security/

III. Data Integrity

A. Backup

B. Disaster Recovery

Integrity – Backup

- Store all data at on-premise servers or in the Cloud (rather than on workstations)
- Deploy data-backup plan:
  - Who manages the process
  - Define where and how backups are stored offsite
  - What gets backed-up (server image, folders, files)
  - How often do backups run (continuous, periodically)
- Get our free 2014 Data-Backup Guidelines at http://www.Bryley.com/Bryley-Data-Backup-Guidelines-2014/

Integrity – Disaster Recovery

- Build/ensure appropriate levels of redundancy in all business-critical systems:
  - Phone system
  - Cloud Services
  - Computer network
- Create and distribute a contingency plan:
  - What offsite resources are available where
  - Who does what, where, and when
- Test often; especially restoration of backups

Get into the Cloud
Safely and Securely

bryleysystems®
MANAGED IT SERVICES
Manage • Optimize • Secure – Since 1987™

Bryley Systems Inc.

Gavin H. Livingstone

- President, Bryley Systems Inc.
- Over 30 years in computer support
- MBA from Boston College, Novell CNE, Microsoft MCSE

Bryley Systems is a full-service partner, fulfilling the information-technology needs of our clients throughout central New England since 1987.

Visit www.Bryley.com for more information.

Synopsis

Cloud Services and your data; learn how to select from Cloud options while protecting yourself from internal and external threats:

- How to compare popular Cloud Services
- Preventative measures to secure your Cloud Services
- How to ensure the integrity of your valuable data, whether inside your office or out in the Cloud

Agenda

I. Comparing Cloud Services
   - A. Going to the Cloud
   - B. Cloud Computing Service Models
   - C. Public, Private, and Hybrid Clouds
   - D. Common SaaS Cloud Services
   - E. Selection Process
   - F. Securing Cloud Services

II. Preventative Measures
   - A. Computer and Internet/Cloud-Use policy
   - B. Security Policy
   - C. User Education
   - D. Technologies

III. Data Integrity
   - A. Backup
   - B. Disaster Recovery

I. Comparing Cloud Services

A. Going to the Cloud
B. Cloud Computing Service Models
C. Public, Private, and Hybrid Clouds
D. Common SaaS Cloud Services
E. Selection Process
F. Securing Cloud Services

Going to the Cloud

- Benefits:
  - Eliminate up-front capital expenditure
  - Reduce operating costs
  - Access from anywhere
- Considerations:
  - Ensure sufficient bandwidth, both up and down
  - Consider Internet fail-over to ensure availability
  - Most start small and expand gradually

Cloud Computing Service Models

- Software as a Service (SaaS):
  - On-demand software; software and data hosted in Cloud
  - Common applications: CRM, ERP, HRM, accounting, etc.
  - Web-based interface with subscription fee per user
- Platform as a Service (PaaS):
  - Basic components (virtual machines, software) to build on
  - Consumer creates the software
- Infrastructure as a Service (IaaS):
  - Raw infrastructure (computing hardware, storage, etc.)
  - Consumer deploys servers and creates entire environment

Public, Private, and Hybrid Clouds

- Public Cloud – Cloud-based resources available to anyone
- Private Cloud – Dedicated Cloud environment:
  - Hosted services to a limited number of people
  - Usually exclusive Virtual Machine(s)
  - Protected behind a firewall
  - Often accessed via VPN
- Hybrid – Interfaced Cloud Services:
  - Combination of two or more Clouds (Private, Public)
  - Often refers to mix of on-premise plus Cloud-based resources (two layer)

Go to http://www.Bryley.com/Hosted-Cloud-Server/ for details on Bryley's Hosted Cloud Server, our private-cloud service.

Common SaaS Cloud Services

- Prevention
- Productivity Suites
- Storage
- Backup and Recovery

Visit http://www.Bryley.com/Solutions/Cloud-Computing/ to see our Cloud Services.

SaaS – Prevention

- Most organizations start with Prevention
- Primary options within Prevention:
  - Email protection – Controls spam plus offers email encryption and archiving
  - End-point security – Secure end-user computers against external attacks
  - Web filtering – Prevent/log unauthorized access to undesired websites
- Popular email-protection options include:
  - McAfee Email Protection – Continuity & Outbound at $27/user per year
  - Microsoft Exchange Online Protection – Exchange only at $12/user per year
  - ProofPoint Essentials Business – Outbound & spooling at $26.40/user per year
- Endpoint security from McAfee, Symantec, AVG, Kaspersky
- Web filtering from McAfee, Axway (Tumbleweed), WebSense
- See http://www.Bryley.com/McAfee-SaaS/ for McAfee options
- We also offer secure transfer: http://www.Bryley.com/Leapfile/

SaaS – Productivity Suites

- Suite of word processing, spreadsheet, slideshow, calendar, email, storage, and other applications
- Google Apps for Business:
  - $50/user per year
  - One size fits all across multiple devices
- Microsoft Office 365:
  - Options start at $48/year, but common at $96/year and up
  - Greater functionality with familiar interface
  - Primarily Windows-based devices
  - Visit http://www.Bryley.com/Office365/

SaaS – Storage

- Desired features (often found only in paid versions):
  - Plans start at $5/user per month; price increases with features & space
  - File synchronization across multiple devices
  - Security with rotating encryption keys
  - Access control and auditing
  - AD/LDAP integration
- Popular options include:
  - Box.net – 10Gb free; highly secure and comprehensive (integration, access control, etc.) offering. Also, NetSkope second-highest rating.
  - Dropbox – 2Gb free; over 200M subscribers. Easiest and most fun to use, but a bit more expensive than comparable offerings.
  - Google Drive – 15Gb free; no frills, but very reliable at reasonable cost.
  - Microsoft OneDrive – 7Gb free; offers the most for the least. Includes unique “Fetch” (from a PC) feature and integrates within MS Office.

SaaS – Backup and Recovery

- Desired features:
  - Automatically copy image or folders and files to Cloud periodically
  - Secure via encryption and somewhat resistant to attack
  - Held separately, unchanged, for recovery purposes
- Popular options include:
  - Carbonite – Extremely popular; automated, encrypted, and easy to use. Starts at $59.99/device per year; business plans start at $299.99/year.
  - Mozy – Well-known with both home and business versions. Home starts at $5.99/device per month; business plans start at $26.98/month.
  - SOS Online Backup – Includes monitoring, password encryption, and phone support. Pricing at $9.99/user per month; unlimited users and devices at $99.99 per month.
- Bryley BU/DR at http://www.Bryley.com/Backup-Data-Recovery

Selection Process

- Primary concerns:
  - Privacy – Based on type of encryption:
    - How are they protecting your data?
    - What tools are used to protect data from third-party access?
  - Resiliency – Measure dependability of the vendor's service via SLA:
    - How much downtime? Conversely, how much uptime (five 9s) or availability?
    - What protocols in-place during downtime? Any remuneration if SLA not met?
  - Customization – What to move to the Cloud and when:
    - Can vendor support a two-layered approach (on-premise plus Cloud)?
    - Can the vendor scale to your needs?
  - Control – More control can reduce Total Cost of Ownership:
    - What can I configure and manage myself through policies via the admin interface?
    - What is no longer available to me?
  - Support – Essential for satisfaction, security, and when things go wrong

Details at http://www.eweek.com/c/a/Cloud-Computing/How-to-Assess-CloudBased-EMail-Security-Vendors/.

Selection Process (continued)

- Key issues:
  - Administration – Easy setup and enforcement
  - Effectiveness – Works reliably and consistently
  - End-user interface – Intuitive, secure, and friendly
  - Granularity – Allows multi-level policies and permissions

Securing Cloud Services

Top 9 threats to Cloud Services in 2013:

1. Data breach – Usually externally, but internal assistance
2. Data loss – Disaster, malware, or lost encryption key
3. Hijacking – Account or service traffic
4. Insecure interfaces and APIs – Awareness
5. Denial of Service (DoS) – Slows performance; increase cost
6. Malicious insiders – Unnecessary access, bad passwords
7. Cloud abuse – Using Cloud computing malevolently
8. Insufficient due diligence – Understand the risks
9. Shared technologies – Shared infrastructure and platform

Visit http://www.Infoworld.com/t/Cloud-Security/9-top-threats-cloud-computing-security-213428.

Securing Cloud Services (cont.)

- Cloud Services provider:
  - Proper provisioning and deployment of Virtual Machines
  - Multi-level security at all points of entry
  - Secure access
- Your habits should include:
  - Proper policies and Internet/Cloud-use procedures
  - Remote backup separate from other services
  - Two-factor authentication where available
  - Preventative measures
  - Disaster Recovery plan

II. Preventative Measures

A. Computer and Internet/Cloud-Use Policy

B. Security Policy

C. User Education

D. Technologies

Preventative – Computer and Internet/Cloud-Use Policy

- Defines how employees use computer and Internet (Cloud) while reducing organization's liability
- Should be as formal as other policy documents
- Objectives:
  - Reduce or eliminate unproductive use (personal shopping, entertainment, etc.)
  - Prohibit illegal use (downloading copyrighted materials, gambling, pornography, etc.)
  - Limit legal liability (sexual harassment, illegal activities)

Preventative – Computer and Internet/Cloud-Use Policy (continued)

- Include within Employee Manual
- Require separate sign-off
- Some suggestions:
  - Use only company-provided Cloud Services
  - Use only company-approved software
  - Do not share accounts and passwords
  - Restrict to business-use only

Preventative – Security Policy

- Complements Computer & Internet/Cloud-Use policy
- Defines, from a technology standpoint, what is allowed and not allowed in the Cloud and on the local network
- Defines the process for making changes, including who authorizes these changes
- Written Security Information Program (WISP)
- Include within Employee Manual
- Require separate sign-off

Preventative – User Education

- Essential to the health of your Cloud Services and your on-premise computer network
- Provide ongoing training:
  - Safe browsing
  - Avoiding phishing and scams
  - Proper password use and storage
  - Do not download viruses and spyware
- Some organizations phish internal users; once hooked, IT provides immediate feedback

Preventative – Technologies

- Operating System
- Firewall
- VPN
- Layering

Technologies – Operating System

- Interface Active Directory or LDAP to Cloud Services
- All users must have own username and password
- Require password complexity with periodic changes
- Use file and directory security to restrict access
- Enable auditing and/or encryption on sensitive data
- Limit administrative access: Administrators use a non-privileged account for day-to-day activities

Technologies – Firewall

- Controls network traffic between its interfaces (typically between local network and Cloud)
- Default rules block most inbound traffic while allowing outbound traffic
- Stateful packet inspection is a required feature
- Universal Threat Management on some appliances
- Automatic circuit fail-over on higher-end models
- See http://www.Bryley.com/Secure-Network/

Technologies – VPN

- Encrypted connection over the Internet
- Primary site requires a VPN-hardware device
- Remote connection can be via a hardware device, login (SSL), or a software client (IPSec)
- Required for Bryley's Hosted Cloud Server; it provides secure connection for Private Cloud

Technologies – Layering

- Create multiple, redundant, levels of protection
- Provide multi-vendor solutions at key areas
- Like home security; the more layers (door locks plus deadbolt, window locks, open/closed sensors, motion sensors, security cameras, etc.) the better.
- Bryley layering for 201 CMR 17.00 compliance:
  - Comprehensive Support Program
  - Secure Network
  - Multi-Point Security Hardening Service
  - Visit http://www.Bryley.com/Solutions/Network-Security/

III. Data Integrity

A. Backup

B. Disaster Recovery

Integrity – Backup

- Store all data at on-premise servers or in the Cloud (rather than on workstations)
- Deploy data-backup plan:
  - Who manages the process
  - Define where and how backups are stored offsite
  - What gets backed-up (server image, folders, files)
  - How often do backups run (continuous, periodically)
- Get our free 2014 Data-Backup Guidelines at http://www.Bryley.com/Bryley-Data-Backup-Guidelines-2014/

Integrity – Disaster Recovery

- Build/ensure appropriate levels of redundancy in all business-critical systems:
  - Phone system
  - Cloud Services
  - Computer network
- Create and distribute a contingency plan:
  - What offsite resources are available where
  - Who does what, where, and when
- Test often; especially restoration of backups

Get into the Cloud
Safely and Securely

bryleysystems®
MANAGED IT SERVICES
Manage • Optimize • Secure – Since 1987™

Bryley Systems Inc.

Gavin H. Livingstone

- President, Bryley Systems Inc.
- Over 30 years in computer support
- MBA from Boston College, Novell CNE, Microsoft MCSE

Bryley Systems is a full-service partner, fulfilling the information-technology needs of our clients throughout central New England since 1987.

Visit www.Bryley.com for more information.

Synopsis

Cloud Services and your data; learn how to select from Cloud options while protecting yourself from internal and external threats:

- How to compare popular Cloud Services
- Preventative measures to secure your Cloud Services
- How to ensure the integrity of your valuable data, whether inside your office or out in the Cloud

Agenda

I. Comparing Cloud Services
   - A. Going to the Cloud
   - B. Cloud Computing Service Models
   - C. Public, Private, and Hybrid Clouds
   - D. Common SaaS Cloud Services
   - E. Selection Process
   - F. Securing Cloud Services

II. Preventative Measures
   - A. Computer and Internet/Cloud-Use policy
   - B. Security Policy
   - C. User Education
   - D. Technologies

III. Data Integrity
   - A. Backup
   - B. Disaster Recovery

I. Comparing Cloud Services

A. Going to the Cloud
B. Cloud Computing Service Models
C. Public, Private, and Hybrid Clouds
D. Common SaaS Cloud Services
E. Selection Process
F. Securing Cloud Services

Going to the Cloud

- Benefits:
  - Eliminate up-front capital expenditure
  - Reduce operating costs
  - Access from anywhere
- Considerations:
  - Ensure sufficient bandwidth, both up and down
  - Consider Internet fail-over to ensure availability
  - Most start small and expand gradually

Cloud Computing Service Models

- Software as a Service (SaaS):
  - On-demand software; software and data hosted in Cloud
  - Common applications: CRM, ERP, HRM, accounting, etc.
  - Web-based interface with subscription fee per user
- Platform as a Service (PaaS):
  - Basic components (virtual machines, software) to build on
  - Consumer creates the software
- Infrastructure as a Service (IaaS):
  - Raw infrastructure (computing hardware, storage, etc.)
  - Consumer deploys servers and creates entire environment

Public, Private, and Hybrid Clouds

- Public Cloud – Cloud-based resources available to anyone
- Private Cloud – Dedicated Cloud environment:
  - Hosted services to a limited number of people
  - Usually exclusive Virtual Machine(s)
  - Protected behind a firewall
  - Often accessed via VPN
- Hybrid – Interfaced Cloud Services:
  - Combination of two or more Clouds (Private, Public)
  - Often refers to mix of on-premise plus Cloud-based resources (two layer)

Go to http://www.Bryley.com/Hosted-Cloud-Server/ for details on Bryley's Hosted Cloud Server, our private-cloud service.

Common SaaS Cloud Services

- Prevention
- Productivity Suites
- Storage
- Backup and Recovery

Visit http://www.Bryley.com/Solutions/Cloud-Computing/ to see our Cloud Services.

SaaS – Prevention

- Most organizations start with Prevention
- Primary options within Prevention:
  - Email protection – Controls spam plus offers email encryption and archiving
  - End-point security – Secure end-user computers against external attacks
  - Web filtering – Prevent/log unauthorized access to undesired websites
- Popular email-protection options include:
  - McAfee Email Protection – Continuity & Outbound at $27/user per year
  - Microsoft Exchange Online Protection – Exchange only at $12/user per year
  - ProofPoint Essentials Business – Outbound & spooling at $26.40/user per year
- Endpoint security from McAfee, Symantec, AVG, Kaspersky
- Web filtering from McAfee, Axway (Tumbleweed), WebSense
- See http://www.Bryley.com/McAfee-SaaS/ for McAfee options
- We also offer secure transfer: http://www.Bryley.com/Leapfile/

SaaS – Productivity Suites

- Suite of word processing, spreadsheet, slideshow, calendar, email, storage, and other applications
- Google Apps for Business:
  - $50/user per year
  - One size fits all across multiple devices
- Microsoft Office 365:
  - Options start at $48/year, but common at $96/year and up
  - Greater functionality with familiar interface
  - Primarily Windows-based devices
  - Visit http://www.Bryley.com/Office365/

SaaS – Storage

- Desired features (often found only in paid versions):
  - Plans start at $5/user per month; price increases with features & space
  - File synchronization across multiple devices
  - Security with rotating encryption keys
  - Access control and auditing
  - AD/LDAP integration
- Popular options include:
  - Box.net – 10Gb free; highly secure and comprehensive (integration, access control, etc.) offering. Also, NetSkope second-highest rating.
  - Dropbox – 2Gb free; over 200M subscribers. Easiest and most fun to use, but a bit more expensive than comparable offerings.
  - Google Drive – 15Gb free; no frills, but very reliable at reasonable cost.
  - Microsoft OneDrive – 7Gb free; offers the most for the least. Includes unique “Fetch” (from a PC) feature and integrates within MS Office.

SaaS – Backup and Recovery

- Desired features:
  - Automatically copy image or folders and files to Cloud periodically
  - Secure via encryption and somewhat resistant to attack
  - Held separately, unchanged, for recovery purposes
- Popular options include:
  - Carbonite – Extremely popular; automated, encrypted, and easy to use. Starts at $59.99/device per year; business plans start at $299.99/year.
  - Mozy – Well-known with both home and business versions. Home starts at $5.99/device per month; business plans start at $26.98/month.
  - SOS Online Backup – Includes monitoring, password encryption, and phone support. Pricing at $9.99/user per month; unlimited users and devices at $99.99 per month.
- Bryley BU/DR at http://www.Bryley.com/Backup-Data-Recovery

Selection Process

- Primary concerns:
  - Privacy – Based on type of encryption:
    - How are they protecting your data?
    - What tools are used to protect data from third-party access?
  - Resiliency – Measure dependability of the vendor's service via SLA:
    - How much downtime? Conversely, how much uptime (five 9s) or availability?
    - What protocols in-place during downtime? Any remuneration if SLA not met?
  - Customization – What to move to the Cloud and when:
    - Can vendor support a two-layered approach (on-premise plus Cloud)?
    - Can the vendor scale to your needs?
  - Control – More control can reduce Total Cost of Ownership:
    - What can I configure and manage myself through policies via the admin interface?
    - What is no longer available to me?
  - Support – Essential for satisfaction, security, and when things go wrong

Details at http://www.eweek.com/c/a/Cloud-Computing/How-to-Assess-CloudBased-EMail-Security-Vendors/.

Selection Process (continued)

- Key issues:
  - Administration – Easy setup and enforcement
  - Effectiveness – Works reliably and consistently
  - End-user interface – Intuitive, secure, and friendly
  - Granularity – Allows multi-level policies and permissions

Securing Cloud Services

Top 9 threats to Cloud Services in 2013:

1. Data breach – Usually externally, but internal assistance
2. Data loss – Disaster, malware, or lost encryption key
3. Hijacking – Account or service traffic
4. Insecure interfaces and APIs – Awareness
5. Denial of Service (DoS) – Slows performance; increase cost
6. Malicious insiders – Unnecessary access, bad passwords
7. Cloud abuse – Using Cloud computing malevolently
8. Insufficient due diligence – Understand the risks
9. Shared technologies – Shared infrastructure and platform

Visit http://www.Infoworld.com/t/Cloud-Security/9-top-threats-cloud-computing-security-213428.

Securing Cloud Services (cont.)

- Cloud Services provider:
  - Proper provisioning and deployment of Virtual Machines
  - Multi-level security at all points of entry
  - Secure access
- Your habits should include:
  - Proper policies and Internet/Cloud-use procedures
  - Remote backup separate from other services
  - Two-factor authentication where available
  - Preventative measures
  - Disaster Recovery plan

II. Preventative Measures

A. Computer and Internet/Cloud-Use Policy

B. Security Policy

C. User Education

D. Technologies

Preventative – Computer and Internet/Cloud-Use Policy

- Defines how employees use computer and Internet (Cloud) while reducing organization's liability
- Should be as formal as other policy documents
- Objectives:
  - Reduce or eliminate unproductive use (personal shopping, entertainment, etc.)
  - Prohibit illegal use (downloading copyrighted materials, gambling, pornography, etc.)
  - Limit legal liability (sexual harassment, illegal activities)

Preventative – Computer and Internet/Cloud-Use Policy (continued)

- Include within Employee Manual
- Require separate sign-off
- Some suggestions:
  - Use only company-provided Cloud Services
  - Use only company-approved software
  - Do not share accounts and passwords
  - Restrict to business-use only

Preventative – Security Policy

- Complements Computer & Internet/Cloud-Use policy
- Defines, from a technology standpoint, what is allowed and not allowed in the Cloud and on the local network
- Defines the process for making changes, including who authorizes these changes
- Written Security Information Program (WISP)
- Include within Employee Manual
- Require separate sign-off

Preventative – User Education

- Essential to the health of your Cloud Services and your on-premise computer network
- Provide ongoing training:
  - Safe browsing
  - Avoiding phishing and scams
  - Proper password use and storage
  - Do not download viruses and spyware
- Some organizations phish internal users; once hooked, IT provides immediate feedback

Preventative – Technologies

- Operating System
- Firewall
- VPN
- Layering

Technologies – Operating System

- Interface Active Directory or LDAP to Cloud Services
- All users must have own username and password
- Require password complexity with periodic changes
- Use file and directory security to restrict access
- Enable auditing and/or encryption on sensitive data
- Limit administrative access: Administrators use a non-privileged account for day-to-day activities

Technologies – Firewall

- Controls network traffic between its interfaces (typically between local network and Cloud)
- Default rules block most inbound traffic while allowing outbound traffic
- Stateful packet inspection is a required feature
- Universal Threat Management on some appliances
- Automatic circuit fail-over on higher-end models
- See http://www.Bryley.com/Secure-Network/

Technologies – VPN

- Encrypted connection over the Internet
- Primary site requires a VPN-hardware device
- Remote connection can be via a hardware device, login (SSL), or a software client (IPSec)
- Required for Bryley's Hosted Cloud Server; it provides secure connection for Private Cloud

Technologies – Layering

- Create multiple, redundant, levels of protection
- Provide multi-vendor solutions at key areas
- Like home security; the more layers (door locks plus deadbolt, window locks, open/closed sensors, motion sensors, security cameras, etc.) the better.
- Bryley layering for 201 CMR 17.00 compliance:
  - Comprehensive Support Program
  - Secure Network
  - Multi-Point Security Hardening Service
  - Visit http://www.Bryley.com/Solutions/Network-Security/

III. Data Integrity

A. Backup

B. Disaster Recovery

Integrity – Backup

- Store all data at on-premise servers or in the Cloud (rather than on workstations)
- Deploy data-backup plan:
  - Who manages the process
  - Define where and how backups are stored offsite
  - What gets backed-up (server image, folders, files)
  - How often do backups run (continuous, periodically)
- Get our free 2014 Data-Backup Guidelines at http://www.Bryley.com/Bryley-Data-Backup-Guidelines-2014/

Integrity – Disaster Recovery

- Build/ensure appropriate levels of redundancy in all business-critical systems:
  - Phone system
  - Cloud Services
  - Computer network
- Create and distribute a contingency plan:
  - What offsite resources are available where
  - Who does what, where, and when
- Test often; especially restoration of backups

