NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | #cybersummitmn

Third Party Risk Management (TPRM) for Small Business

Chuck Pellino – Managing Security Architect – Information Security

Wells Fargo - Charles.e.pellino@wellsfargo.com

University of Minnesota TLI – MSST class of 2012

Agenda

Review common Cyber security controls and capabilities assessed and required of Third party providers by Enterprises. Deployment of these capabilities does become a business enabler and often differentiates one small businesses from another. The Red Tape!

Fraud Trends: Business Email Compromise (BEC) / Email Account Compromise (EAC), Account Take-Over (ATO) and other increasing fraud in financial transactions.

Third Party Risk Management roles for any size business

1. Third Party Service Provider, Supplier, Business Associate, to another business or entity
2. Consumer of Third party solutions; every business has multiple third party relationships
    1. IT and Service providers (SaaS)
    2. Third party hosting services (IaaS, PaaS)

Why all the Red Tape!

1. Financial and other regulatory requirements for managing Third Parties, OCC, FDIC, SEC, PCI, GLBA, FTC, HIPAA, SWIFT
2. Risks of compromise through vendors and trusted third parties is increasing: Island hopping, and lateral movement to partners

Regulatory Requirements: FDIC

"The board of directors and management of an insured depository institution (institution) are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution."

https://www.fdic.gov/regulations/compliance/manual/7/vii-4.1.pdf

Regulatory Requirements: OCC

“The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.”

https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

The Red Tape: Initial TPHS Assessments and Red Flags

1. Identity Management and Federation
2. Tenancy
3. Network Architecture
4. Data protection in Flight and Rest
5. Key Management (HSM)
6. Vulnerability Management
7. Industry Certifications

Identity Management and Federation

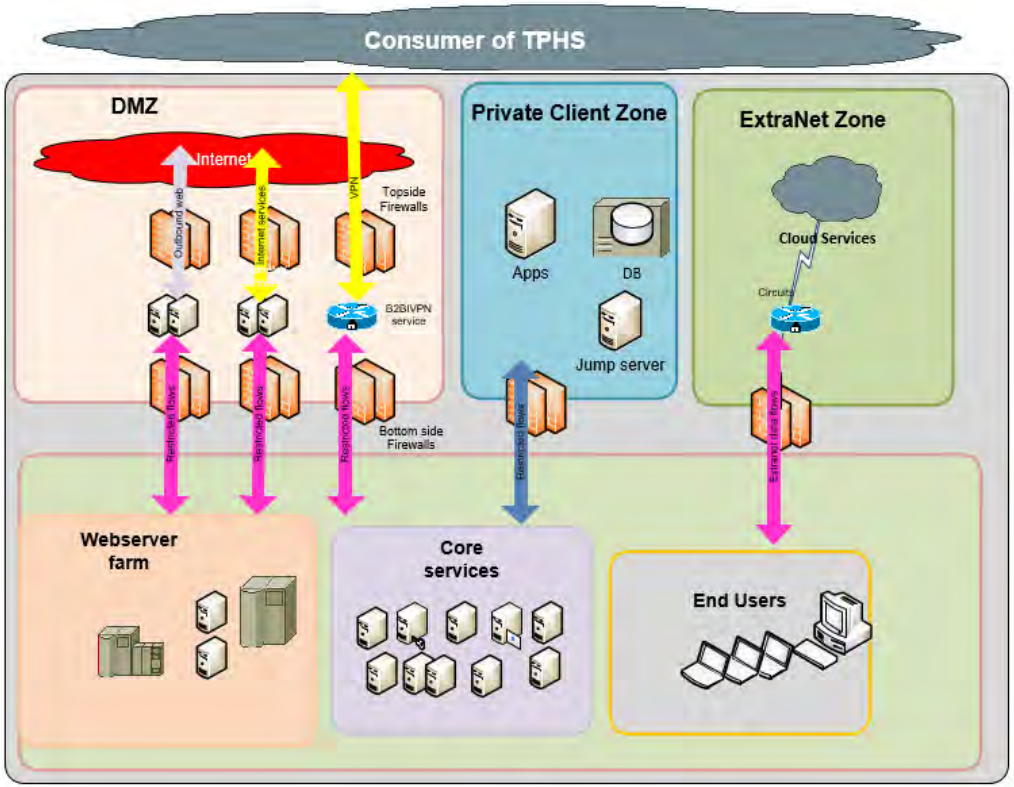
- Authorization
  - How is fine-grained authorization for your data handled
- Privileged account management
  - 2FA is required for Privileged accounts
  - 2FA is required for Remote access 
- Id Federation is always required
  - SAML 2.0 most often utilized and supported
  - Allow you to manage your users
- Local Administrator accounts

Tenancy

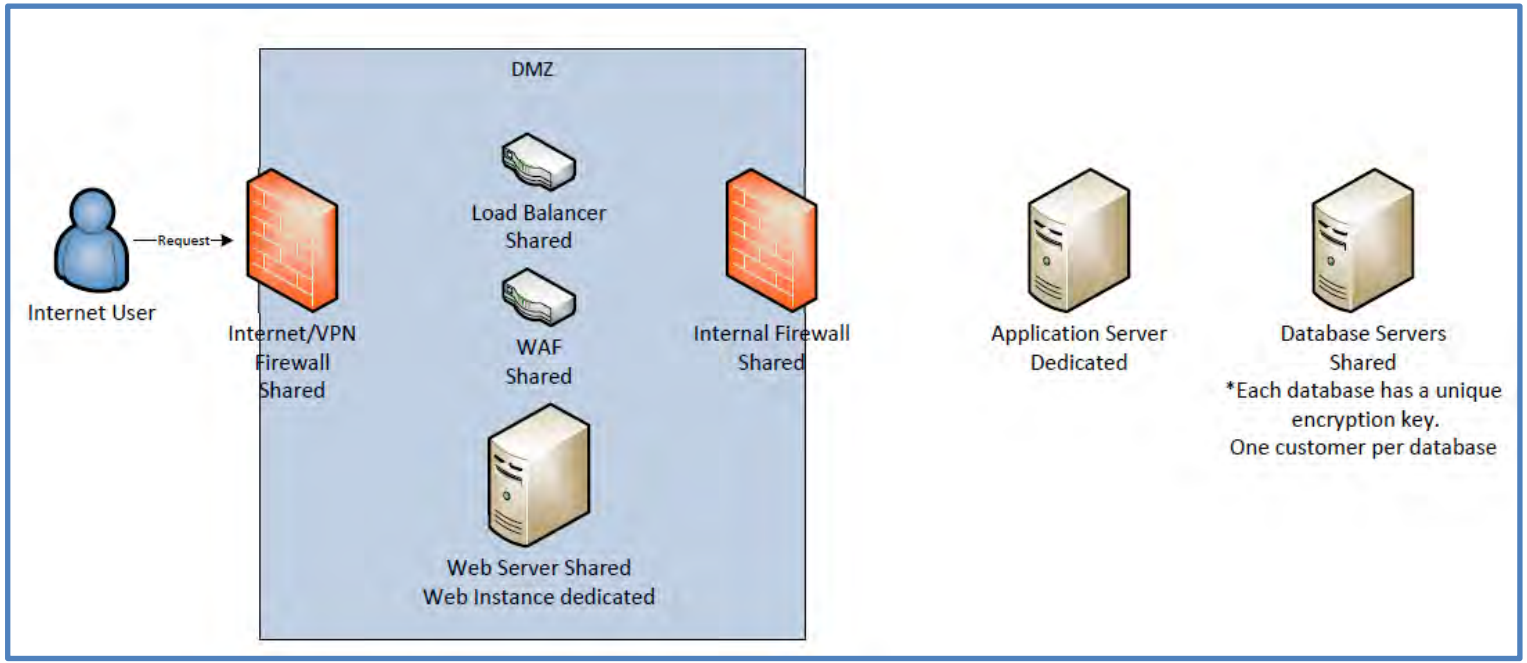
- Sensitivity of the data (PII, PCI etc.) drives the requirements
- Single or multitenant environments
- Logical or physical
- Cloud responsibility models

Network Architecture

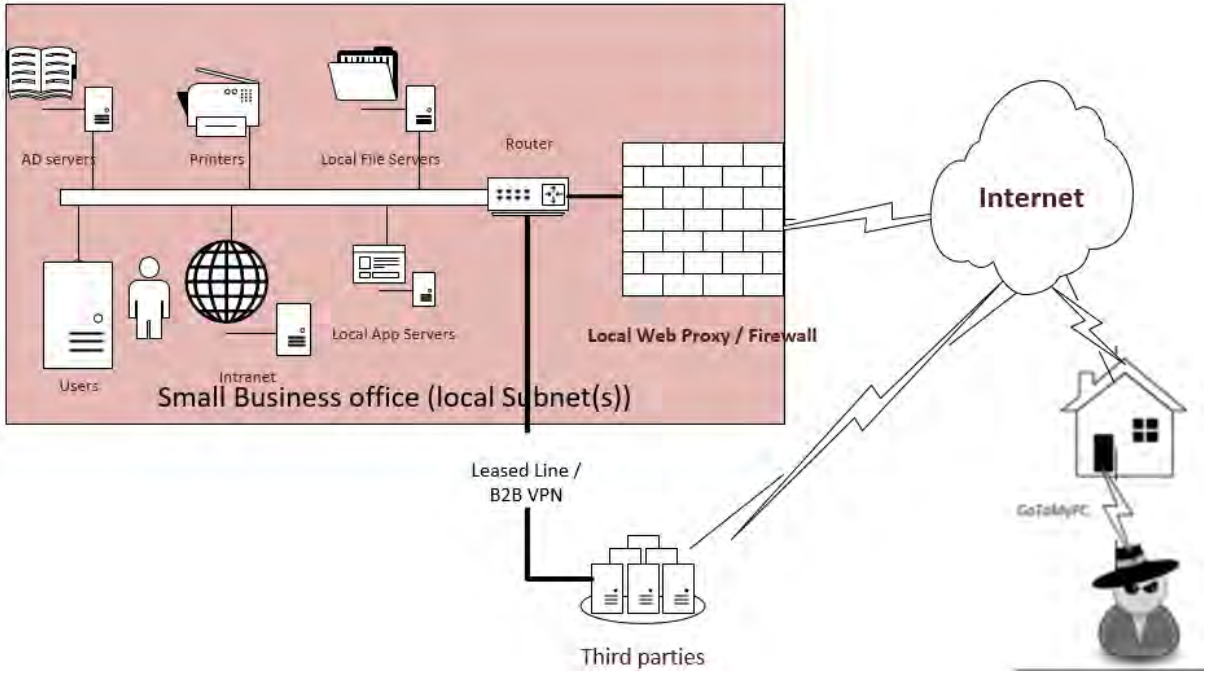
- Segmentation
- DMZ design (WAF, IDS, DDoS, Firewall)
- Redundancy
- Remote Access



Network Architecture



Network Architecture: Remote Access



Attackers utilize common remote access tools to gain access to networks

- GoToMyPC
- RDP Microsoft
- TeamViewer used by support firms
- Webex, goToMeeting, others
- PC Anyware
- Dameware
- VPNs from soft targets

Creates a bridge to the attacker by passes Firewalls

Data Protection in Flight

- TLS 1.2 and higher is the standard, PFS
- Encryption in flight is required end to end
- Mutually authenticated TLS is required for node to node
- B2B VPNs are preferred over Internet transport. (Internet facing opens up more requirements)
- SSLlabs.com “A”

Data Protection at Rest

- All end user computers employ Full Disk Encryption
- All Data must be encrypted at rest
- Databases storing confidential data require encryption protections above storage level or hardware level
- Manage and store passwords and pins using strong hash cryptographic algorithms, protocols, and tools (use ID Fed)

Key Management

- A Key Management solution is required for full life cycle management of cryptographic keys on Hardware Security Modules (HSM)
- Product's NIST CMVP FIPS 140-2 or other NIST validation status, level, and certificate number
- Full assessment often required dependent on data classification level hosted by third party

Vulnerability and Patch Management

A formal vulnerability and patch management program is required to ensure application, system, and network device vulnerabilities are evaluated, and patches applied in a timely manner (based on CVSS or equivalent)

Security patches must be installed promptly:

- Emergency 3 days; Think Struts!
- High - 30 days

SAST, DAST and MPT

- Required for all Internet accessible applications
  - Static Application Security Testing (SAST)
  - Dynamic Application Security Testing (DAST)
- Most often required
  - Manual Penetration Testing (MPT)

Note: Third Party assessors can be utilized to protect IP

Industry Certifications

- SOC 1 (SSAE18) independent audit annually
- SOC 2/3 (Trust Services Criteria) independent audit annually
- ISO/IEC 27001:2013
- FedRamp ATO or tenant
- HIPAA certified
- PCI compliant (Level 3)
- TRUSTe Privacy certified
- GDPR Compliant
- EU & Swiss – U.S. Privacy Shield certified

Fraud Trends

Impersonation Attacks

- Business Email Compromise
- Tech Support Scams (ATO)
- Account Takeover (ATO)

The 2018 Internet Crime Report emphasizes the IC3's efforts in monitoring trending scams such as Business Email Compromise (BEC), Extortion, Tech Support Fraud, and Payroll Diversion. In 2018, IC3 received a total of 351,936 complaints with losses exceeding $2.7 Billion.

https://pdf.ic3.gov/2018_IC3Report.pdf

Business Email Compromise (BEC)

Types of Imposter Attacks

- **Executive Imposter-** Fraudster posing as an executive of the company, such as the controller or CEO, instructs an accounts payable clerk to make one or more payments

- **Vendor Imposter-** a fraudster posing as a vendor request change to the vendor's payment instructions

- **W2 / HR Fraud** –a fraudster posing as an executive of the company request W2, deposit or employee or customer PII information

Business Email Compromise (BEC)

Fraudster poses as a trusted person or entity, typically a senior executive or a vendor partner

Fraudster sends instructions via email, phone, fax, mail and requests a payment or asks to change bank information for the vendor's payment instructions

The finance / accounting staff complies with the payment instructions and makes the payment using their normal payment channel and bank

Bank receives the payment instructions from the customer and executes the funds transfer based on those properly authenticated instructions

In 2018, the IC3 received 20,373 BEC/E-mail Account Compromise (EAC) complaints with adjusted losses of over $1.2 billion

https://pdf.ic3.gov/2018_IC3Report.pdf

Business Email Compromise (BEC) : Payroll

Large School District payroll received an email from who they thought was the school district Superintendent

Fraudster asks to change Superintendent banking details and override the pre-notification for his payroll direct deposit

Fraudster asked for a copy of the direct deposit form. Payroll obliged. The fraudster returned the filled-out form along with a bogus check—by email

Payroll updates the direct deposit for the Superintendent who discovers loss on Payday

100 complaints with a combined reported loss of $100M in 2018. (IC3)

https://digital.wf.com/treasuryinsights/portfolio-items/tm6039/

https://pdf.ic3.gov/2018_IC3Report.pdf

Business Email Compromise (BEC): Prevention

Be vigilant, and implement the following best practices:

- Stay alert for requests to change vendor payment information or instructions.
- Verify the requestor with a phone call, email, or both if appropriate, **using the contact information you have on file.**
  - If the request was received by mail, fax, or email, verify it with a phone call.
  - If the request was received by phone, verify it by email.
- Monitor account activity for unauthorized or unusual activity.
- Protect your email account and devices
- Use **dual custody <u>properly</u>** to verify payment details before they're sent.
  - Dual custody requires that online payment transactions or administrative changes initiated by one user be approved by a second user on a different computer or mobile device.

https://www.wellsfargo.com/com/ceo/ceo-mobile-banking/

Tech Support Scam: Using Dual Custody and 2FA incorrectly

Customer attempts to logon into a portal and is prompted for credential to include token code, but has difficult logging in.

Shortly after, user will receive a call from person claiming to be from the bank, and offers to assist with the login issues. This Fraudster requests that a second person is needed to login in order to troubleshoot the issues.

User complies and asks a manager to sign in on that computer; user enters credentials including token code. They are advised that problem will be resolved in 15 minutes and that they should wait before accessing the portal.

What happens next? Wire transfer using both sets of credentials.

In 2018, the IC3 received 14,408 complaints … amounted to nearly $39 million, which represents a 161% increase in losses from 2017.

Business Email Compromise (BEC): Identifying

Check for red flags: include, but aren't limited to:

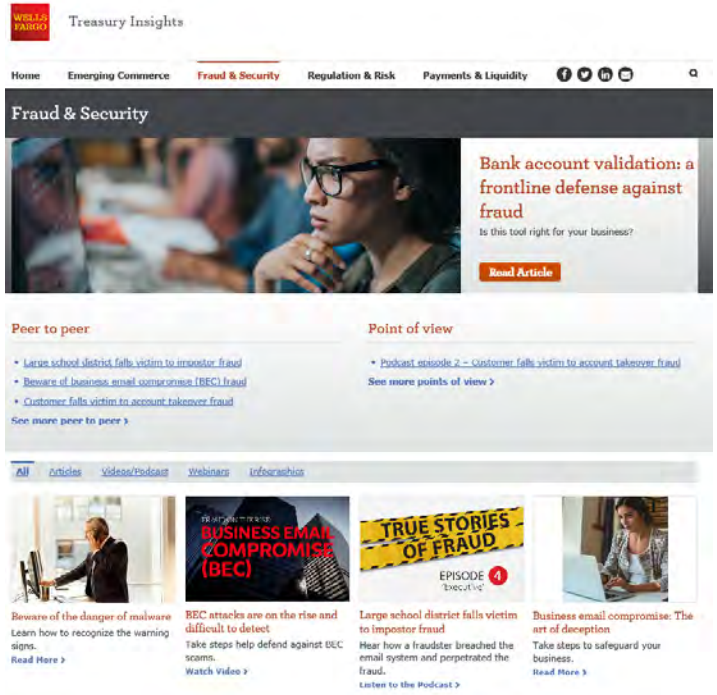
- High degree of urgency
- Request to keep the payment confidential
- Switching from a commercial beneficiary to an individual beneficiary
- Changing from an organization's email domain
- Subtle changes to the organization's name
- Payment amount doesn't match the invoice or request
- Name, mailing address, or account number don't match the information you have on file.

Business Email Compromise (BEC): Dual Custody

Use dual custody as it's intended to be used- no rubber stamps or payment fast tracks

- Dual Custody gives you a second chance to spot a fraudulent payment before it goes out the door.
- Both the payment initiator and the approver must pay close attention to the payment details
  - Initiator – Verify before you initiate, use a checklist to ensure key details are reviewed
  - Approver- Verity before you approve. Do not trust the initiator's verification or assume the payment is appropriate because you recognize part of the information
- Processes that rely on a single channel such as email will fail

Business Email Compromise (BEC): Training Resources



Wells Fargo Treasury Services: Fraud and Security
https://digital.wf.com/treasuryinsights/fraud-security/

FBI: Internet Crime Complaints Center https://www.ic3.gov

Account Takeover – Man in the Browser

Send malicious attachment in email to infect end users computer or smart phone

Or, Gain control of an ad network or website to create a watering hole

Malware installed on end-users device and monitors access to banking, Email or other targeted sites

Keyloggers capture user credentials to be reused by attacker.

Or, User web request is redirected to a fake site where credentials are captured when entered and passed to the real website.

Attacker issues legitimate credentials to the real website acting as the customer potentially triggering an SMS or email authorization code

Account Takeover – Man in the Browser Cont.

The SMS code or email delivered code is presented to the fake website. Credentials are captured when entered and passed to the real website

Accounts are compromised. Other websites are accessed if the user reused the username and password. Credential stuffing

Introduce Dual Custody especially for high dollar transactions

Account Takeover – Prevention

- Dual Custody prevents the compromise of single device
- Harden payment workstations as you would your administrators
  - Browser sandboxes or whitelists
  - VDIs or separate single purpose workstations for payment operators
  - Privileged Accounts for Payments
  - Enhanced logging and monitoring
  - 2FA
- Consider adding ACH Debit blocks and utilize Proxy account numbers (payment identification codes) for Receiving customer payments (check with your banker)

Account Takeover – Prevention

- **Explore implementing account verification services**
  - **Account status.** Confirms that a deposit account is open and valid, and assesses the risk of items being returned.
  - **Account status and ownership.** Allows you determine if your client is a designated signatory with authorization to transact on an account. This service is available for those banks that contribute account ownership information. (2600)
- **Train your staff and partners**
  - Authenticating payment requests
  - Educating executives and staff about the threat of fraud
  - Instructing staff to question unusual payment or account requests received by email; Time matters!
  - Providing awareness to vendors and trading partners on the threat of fraud and the process for communicating about financial transactions and information

Looking forward – Trends and Predictions

- BEC continues to expand
  - More government based spoofing
  - VEC grows for lateral movement
- Extortion continues
  - Paying the Criminals to get your data back will not be an option
    - OFAC
    - Money laundering

Thank You