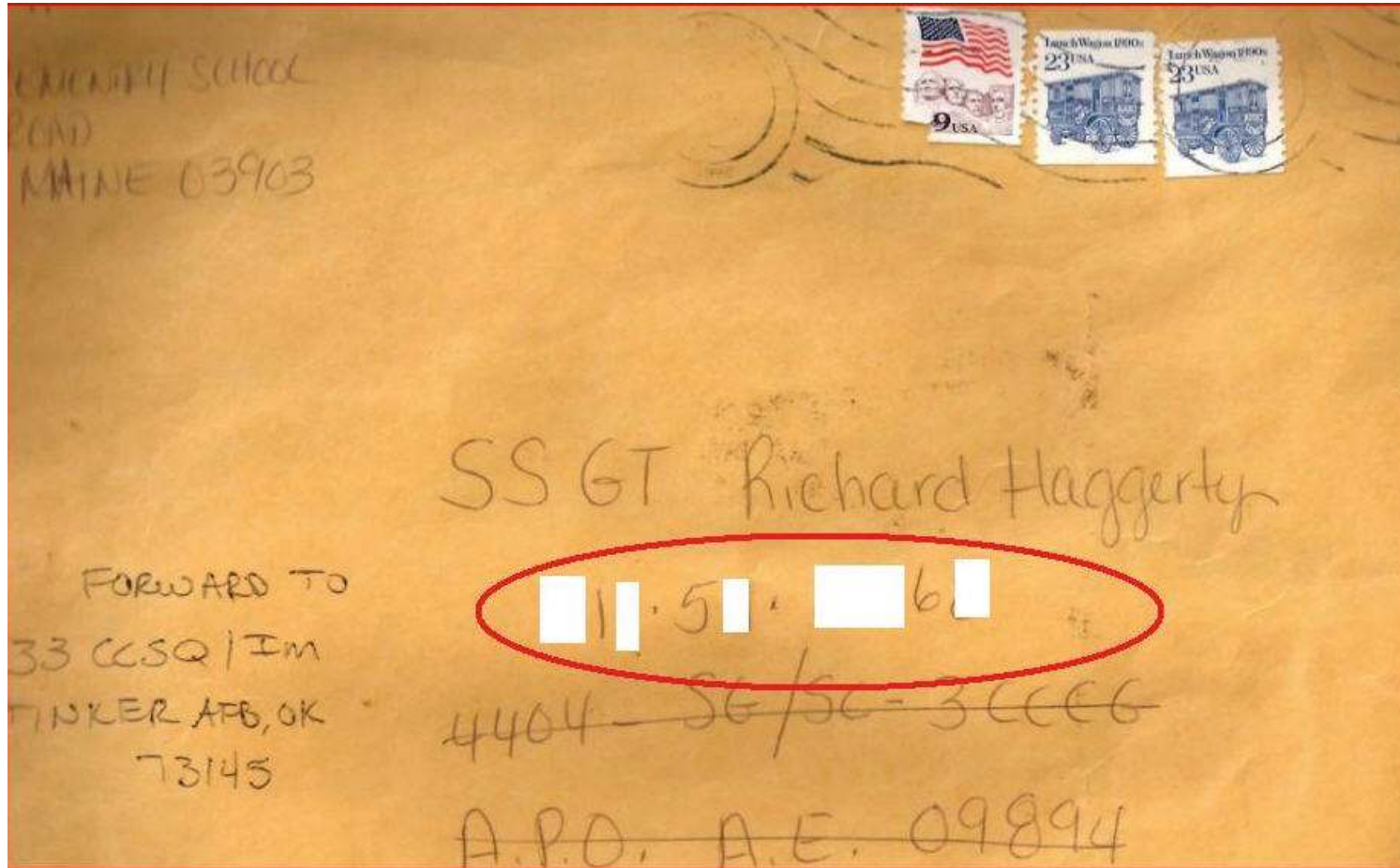


Third Party Data Security

Rich Haggerty
CISM, CISA

Mail Call



My SSN was used as part of addressing mail (1991)



Today-“The Envelope Window = Lawyers”

I received my stock trading account statement in the mail from my stock trader

- SSN was visible in the window of the envelope
- I called my broker to explain the risk/error
 - They handled it professionally and took it seriously
- I'm still not very happy with my broker
- Several weeks later, I get a letter from the brokers print vendor

The letter stated that the broker was not at fault. The print vendor was fully responsible for the error. They had a mix up in the type of envelope to use for that job, which led to the error. They corrected the process to correct the error to prevent it from occurring again.

Can you imagine what type of lawyers/legal discussions were held between the broker and the print vendor that led to the print vendor sending that letter of explanation?

I would imagine the Vendor Due Diligence/Security Groups were involved in this discussion.



Compliance and Security of Customer Data

- FFIEC
- GLBA
- ID theft
- Suspicious Activity Reports
- Laws
- Lawsuits



Gramm-Leach-Bliley Act (GLBA)

Applies to Financial Institutions

- Protect customer data
- Ensure third party security of your customer data

“In order to develop, implement and maintain your information security program, you shall: oversee service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue”

Ref: GLBA sec 314.4.d1



GLBA-Third Party Expectations

“Before entering into outsourcing contracts, and throughout the life of the relationship, institutions should ensure the service providers’ physical and data security standards meet or exceed standards required by the institution”

GLBA Sect 314



GLBA High Level

- Step One: Determines whether the third party is a viable company to conduct business with. Are they a sound company with general controls and appropriate security standards?
- Step Two: Ensure the methods of information sharing is secure and compliant with applicable regulations
- Step Three-make sure steps one and two remain intact

Your company shares the data, it all falls on you.

Are you lucky or good?



Federal Financial Institutions Examination Council (FFIEC)

Federal guidelines regarding technology controls and outsourcing technology services

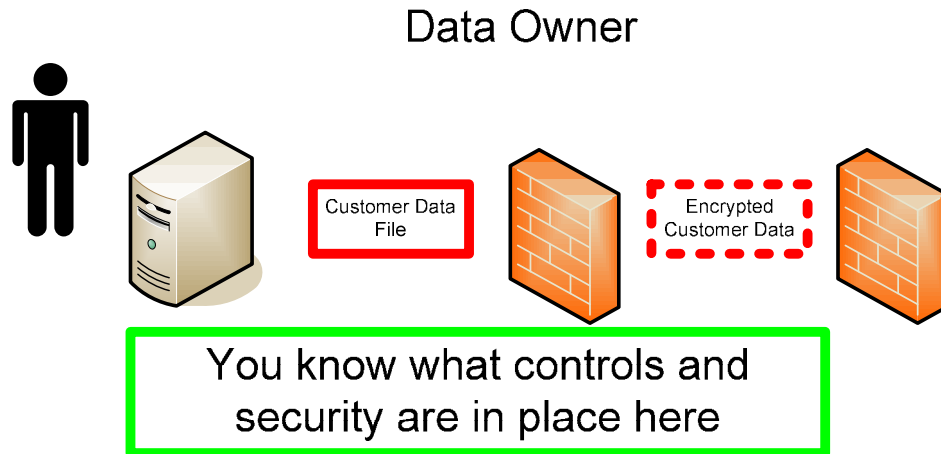
“The organization must monitor its foreign-based service providers to confirm that they have satisfied security obligations imposed in the contract to comply with Section 501(b) of GLBA”

FFIEC Outsourcing Technology Services (2004)

www.ffiec.gov



Where does it end? It doesn't.



Third Party Vendor



You Don't know what happens here, but you need to.

- How is the file handled?
- Is the file sent elsewhere for further processing?
- Is that an outsourced activity?
- Is it in the United States?

<Our Company> - Our Challenge

- Identify and remediate what we thought were about 80 vendors
- Establish process to stop internal issues regarding the handling of customer data
- Establish a sustainable GLB/FFIEC vendor diligence & security program
- Increase vendor security/data protection awareness at all levels of the company



Our Approach in the Beginning: Process-not technology

- Start with Business Leaders?
- Start with IT Leaders?
- Start with Vendor Management?
- Start with A/R & A/P?



Where to begin-continued

We started with our computer operators. They know the batch jobs and what arrives and leaves

Don't overcomplicate or over engineer the remediation

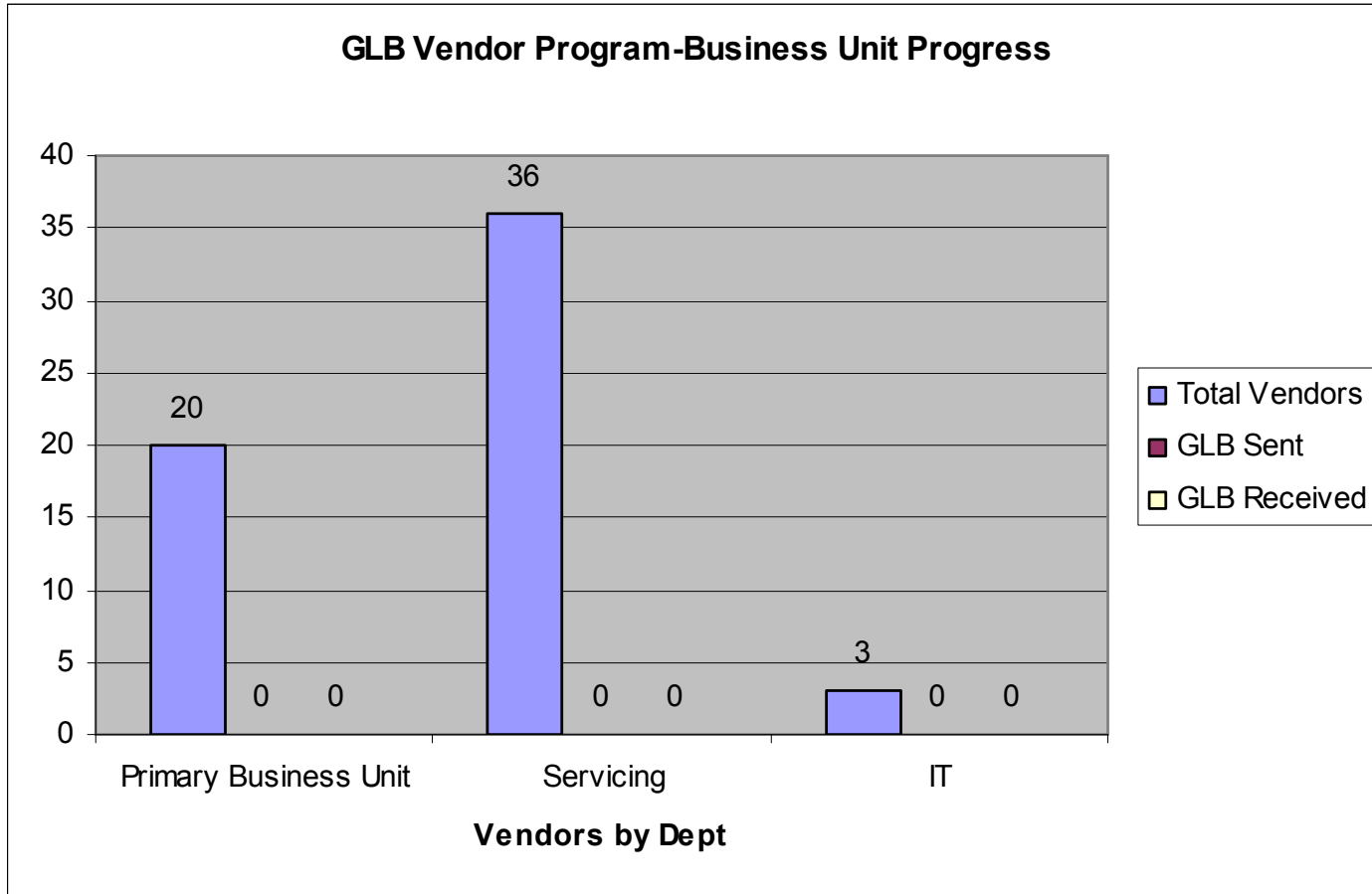


The Vendor List 60 and Tracking it

- MSAccess Database
 - Vendor, NPPI, Encrypted y/n, Notes
- At this point, we had it organized enough to begin the process
- We could sort by business unit and start reaching out to business leaders to push the program
- We thought we had 80, in reality we had 60



Follow up with CIO- Program Remediation Begins



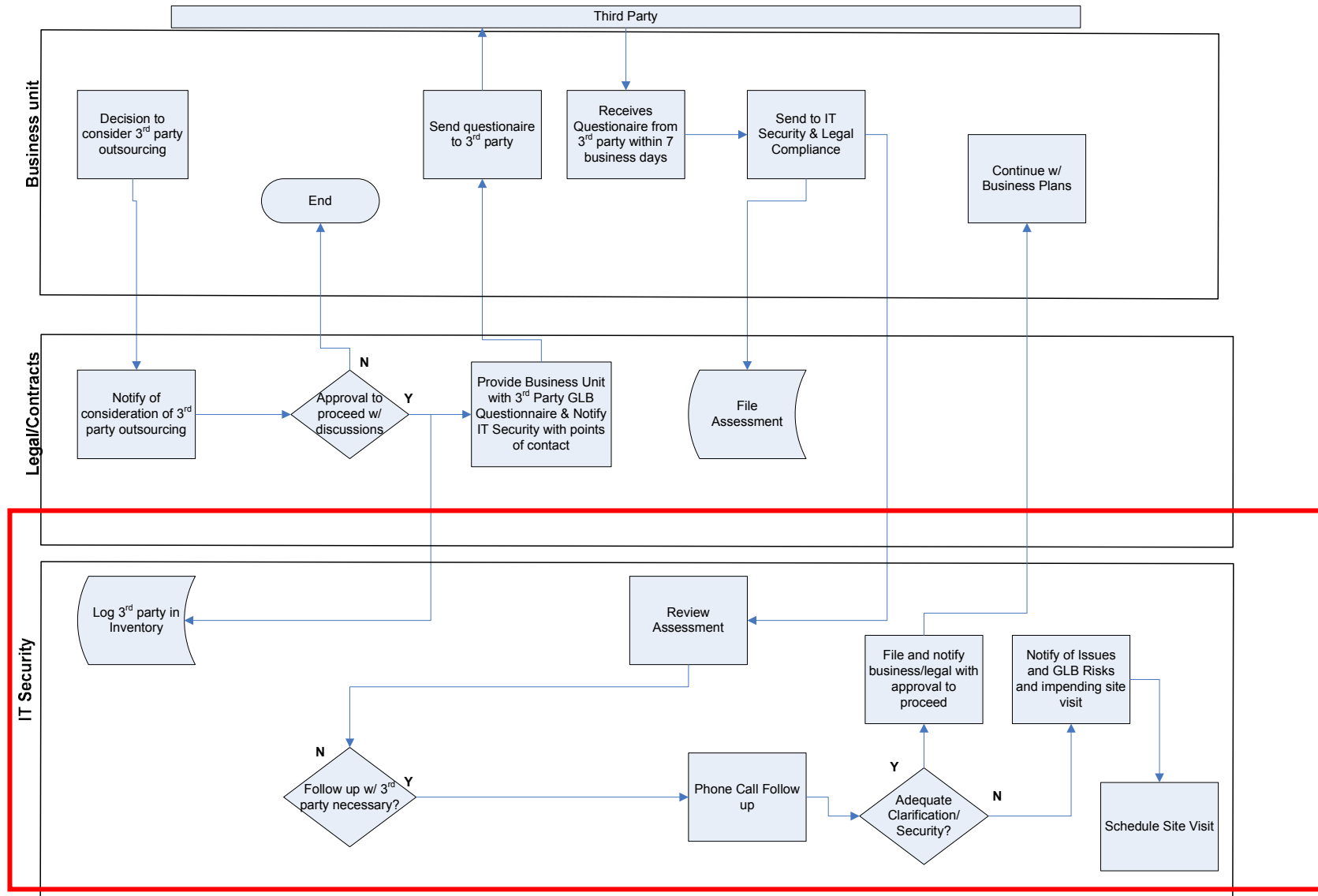
Awareness-The Biggest Bang for Your Buck

- Established a process in our project process to provide early warning to IT operations, Information Security
- Awareness and basic 'rules' for Operations folks
 - Everything gets encrypted
 - File level encryption is mandatory
 - File encryption covers you in many ways
- Internal business leader awareness
 - Vendor contacts and review process
 - Their roles
 - Reporting progress

NOTE: Always get the business contact for the vendor. This accelerates the process.



Outlined Vendor Management Review Process & Procedures



Contacting the vendors

- Standard email to all vendors
 - Contact the vendor business person first (not the IT or Security Group)
 - CC internal business leaders on email
 - Questionnaire attached to email
- Some vendors offer a SAS70. This helps the process.
 - SAS70 must be read as you can't rely on it 100%. All depends on the business relationship of the SAS70 holder



Consistent Email to Vendors

Dear <Insert Name>

Date

<Our Company> is conducting our annual requirement under Gramm-Leach-Bliley (GLB) to ensure adequate information security practices are in place to protect <Our Company> customer data.

The purpose of this questionnaire is for you to provide to <Our Company> information about the practices and safeguards you have in place to protect the security, confidentiality, and integrity of <Our Company> customer or employee nonpublic personal information (“NPI”), which may be provided to you as part of your vendor relationship with <Our Company>.

Please complete this questionnaire with 10 business days of receipt.

If you have any questions regarding this questionnaire, please contact our Information Security department.

Thanks for your cooperation and time in completing this document.

<Our Company> information security team contact information:

E-mail: informationsecurity@<Our Company>

Phone 214-xxx-xxxx



Review of GLB Questionnaires

- Review answers
- Do answers correlate to size of company
 - # employees is a big indicator
 - 4 employees but a full blown DR plan and every privacy policy completed?
- Generally tell when vendors are struggling to provide “The right answer”
- Log notes in MSAccess
- Added field for risks
- File questionnaire on network folder



Vendor follow up

Business involvement-critical

- Inform business leaders of issues that will be discussed with each vendor
 - Invite them to the discussion
- **Ensure the vendor business person is on the call**
- Call vendor and discuss areas needing clarity/explanations



Do you need to visit the site?

- Tier 1 vendor-Mandated
- Tier 2 review risks, data exchanged
- Expertise to decide
- Sometimes you can 'just tell'

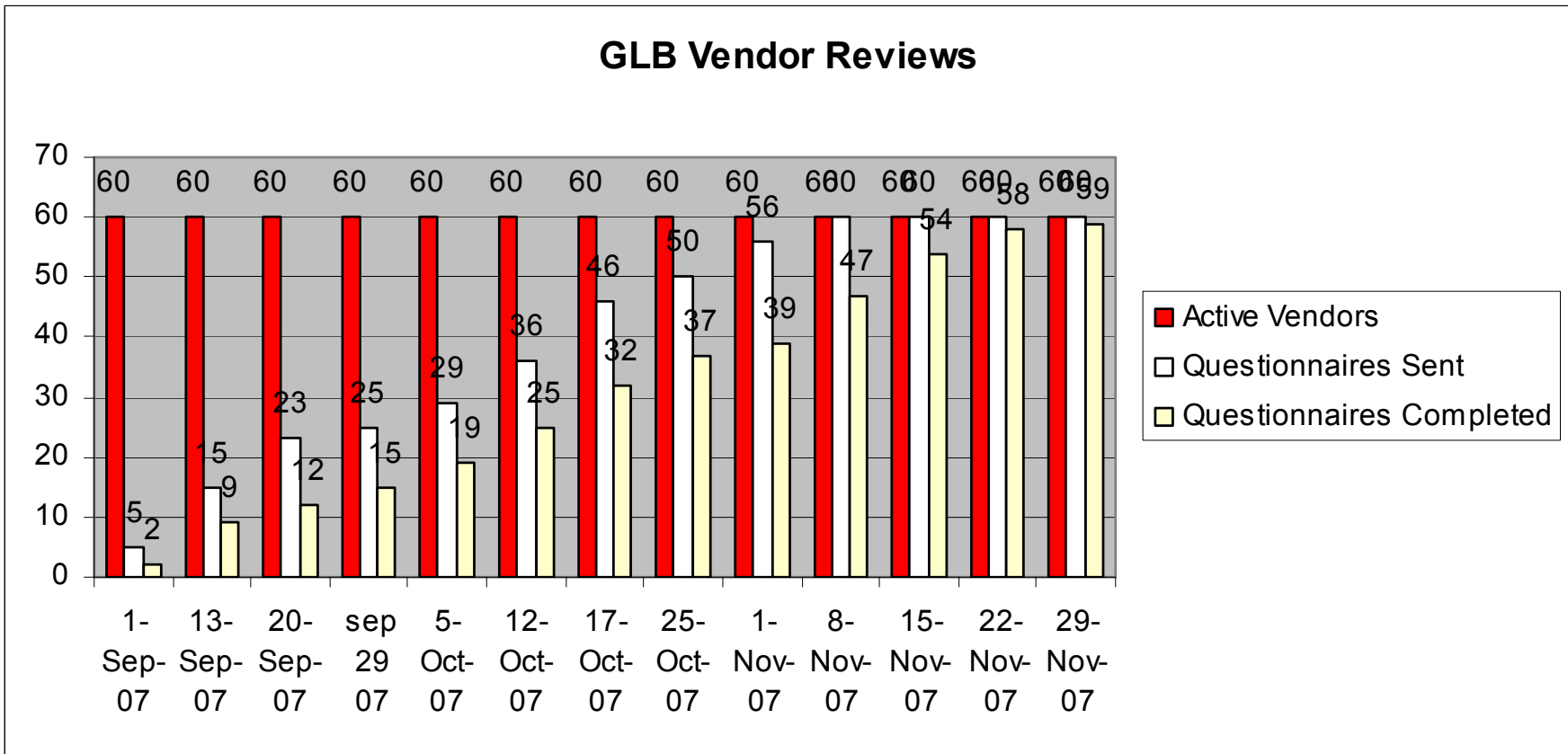


Checking vendors off the list

- MSAccess
- Folder for each vendor with their answered documents and my comments
- Date reviewed
- Continued until complete
- Basic reporting



We saw a slow and steady level of remediation/compliance. In six months time we were out of the woods.



Success- we were compliant

We reached a point to where the solution worked

- We celebrated
- We took a breather
- Slowly, we started to see the processes fray a bit
- We then realized another challenge

What we had would not scale much further



PROCESS changes were not needed. We needed process consistency and centralization.

- Centralized information was needed by other internal groups
- Needed to get away from the documents and emails
 - Important items were getting dropped (emails, tracking etc..)
 - Misc notes were initially good, but started to become inconsistent
- Renewals of vendors were to begin in 6 months
- Internal audit was conducting audits and really pressing on vendor management and due diligence
- My MSAccess skills were bypassed long ago



Invested into a central repository to help facilitate the scale issue

- We utilized the same process but in a more streamline manner
- Our efforts in awareness, process, organization roles were utilized as before
 - The effort was not a waste of time/resources

The tool helped advanced the program by:

- Questionnaires are all online
 - Vendors login, complete and acknowledge the answers
 - We can query based on vendor, answer, response etc..
- Internal comments, reviews, notes are all listed within the system
- Vendor, GLB and Risk were all centralized
 - Expanded process to Compliance and internal controls group
- Reporting, tracking, documenting
- Forecast schedule



Summary

- Process driven, not technology driven
- No silver bullet
- Business involvement is critical
- You are responsible for your customer data wherever it ends up
- Awareness takes time but the payback is exponential to the effort
- Make sure it scales and can work consistently





Rich Haggerty

Information Security Consultant

RichHaggerty@gmail.com