Thomas W. Wilson, Jr.
Scott R. Schaffer
Jonathan E. Meer

August 3 and 4, 2017

Quite a Catch! Phishing for Social Engineering Fraud and Understanding the Importance of Legal Project Management

Presentation for the Rhode Island Bar Association

WILSON ELSER

Focus of Today's Presentation

- Cyber Risks
  - Social Engineering Fraud
  - Ramsomware
  - Lawyers Misuse of Technology
- Law Firm Management & Cyber Risk
- Legal Process Management with focus on Cyber
- Legal Process Improvement

What is a Cyber Attack and Why Should you Care?

- 15% of law firms suffered a cyber attack in 2015
- "'There are only two types of companies,' Mr. Mueller [the head of the Federal Bureau of Investigation] said in a keynote speech at the [RSA] conference, 'those that have been hacked and those that will be.'"
- "[I]f somebody wants to get into your system, they have a very, very good chance of doing it. So if you don't want your system compromised, disconnect it from the Internet. … [T]ake a hammer to the hard drive. At that point, you're relatively secure."

  -- **Philip Reitinger, Department of Homeland Security**

What Type of Law Firm Information Is at Risk?

- Sensitive business data: projections, forecasts, M&A
- Social Security and driver's license numbers
- Medical records
- Financial information: bank/credit card accounts
- Personal information: email addresses, phone numbers and home addresses (if coupled with other information)

Duty of Technological Competence

- RI R.P.C. 1.1 Competence:
  - "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation"
- Comment 8 (not yet adopted in RI):
  - "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, and engage in continuing study and education."

Duty of Technological Competence- RI R.P.C. 1.6

- Rule 1.6. Confidentiality of information:
  - A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, ….
- Comment 18 to Rule 1.6 (Not yet adopted in RI):
  - Factors as to reasonableness of confidentiality efforts include sensitivity of information, likely disclosure if safeguards not taken, costs and difficulty of safeguards, whether safeguards adversely affect the ability to represent clients. A client may require safeguards and can waive these.

Duty of Technological Competence

- E-Discovery
- Electronic filing of court documents
- Communicating with clients and third-parties
- Use of social media
- Knowledge of client's technology
- Use of courtroom technology

RI Identity Theft Protection Act, §11-49.3

- Anyone possessing personal information must implement "reasonable security procedures and practices" to avoid unauthorized access
- No one shall retain personal information for longer than required to provide the services
- Everyone shall destroy all personal information in a secure manner, e.g., shredding or burning

RI Identity Theft Protection Act, §11-49.3

- Everyone who discloses personal information to a third party shall require by written contract that the third party implement and maintain reasonable security procedures and practices to protect unauthorized access

RI Identity Theft Protection Act, §11-49.3

- "Personal information" is first name or initial, and last name with any one of the following:
  - Social security number;
  - Driver's license number;
  - Financial account number with security code, access code, or password that permits access;
  - Medical or health insurance information; or
  - E-mail address with any code would permit access to financial or health account

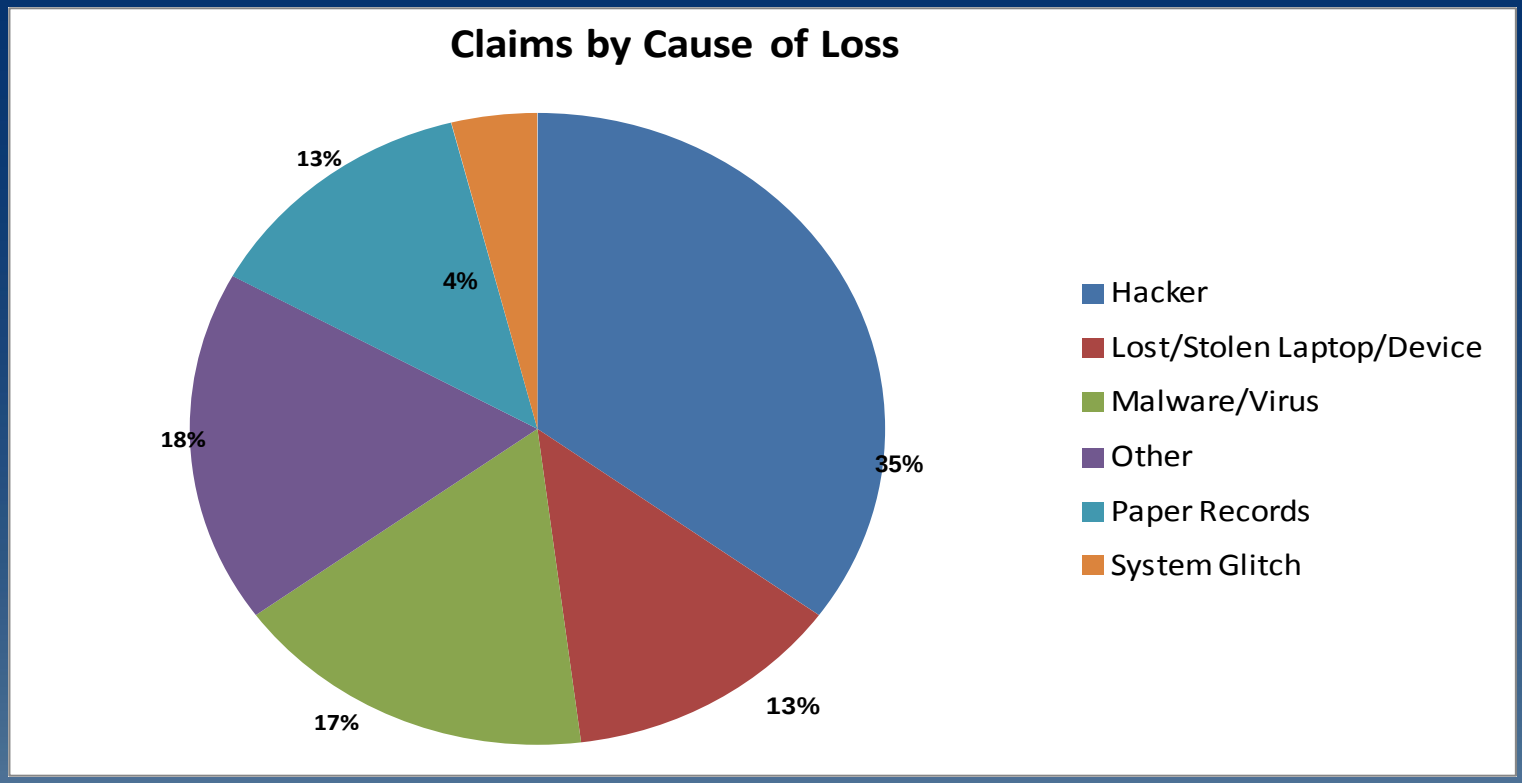
RI Identity Theft Protection Act, §11-49.3

- Notification if "significant risk" of unauthorized access
- 45 days to give notice of significant risk
- Must notify Attorney General and credit reporting agencies if 500+ people involved
- Notice must include how breach occurred, type of information, date of breach and discovery, remediation offered
- Civil penalty of $100/reckless breach per record and $200/knowing and willful breach

Duty of Technological Competence

- Competence does not require perfection
- Encryption generally not required, but RI statute exempts encrypted information
- If you lack competence, talk to others in the firm
- If they do not have competence, hire third-party vendors
- Make sure to advise client and obtain consent for hiring third parties to protect their interests

Causes of Cyber Losses



2016 NetDiligence Cyber Claims Study Report

Threats from Outside the Firm

- Social Engineering Fraud
- Phishing and Smishing
- Ransomware
- Hacking into confidential information
- Other Social Media Exposures

Social Engineering Fraud

- What is Social Engineering
  - Manipulating someone into doing something by clandestine means

- Types of Social Engineering
  - Quid Pro Quo
  - Phishing
  - Baiting
  - Pretexting
  - Diversion Theft

Social Engineering Fraud

- Attacker uses human interaction to obtain or compromise information
- Attacker may appear unassuming or respectable
  - Pretending to be a new employee, repair man, etc.
  - May even offer credentials
- By asking questions, the attacker may piece enough information together to infiltrate an organization's network
  - May attempt to get information from many sources

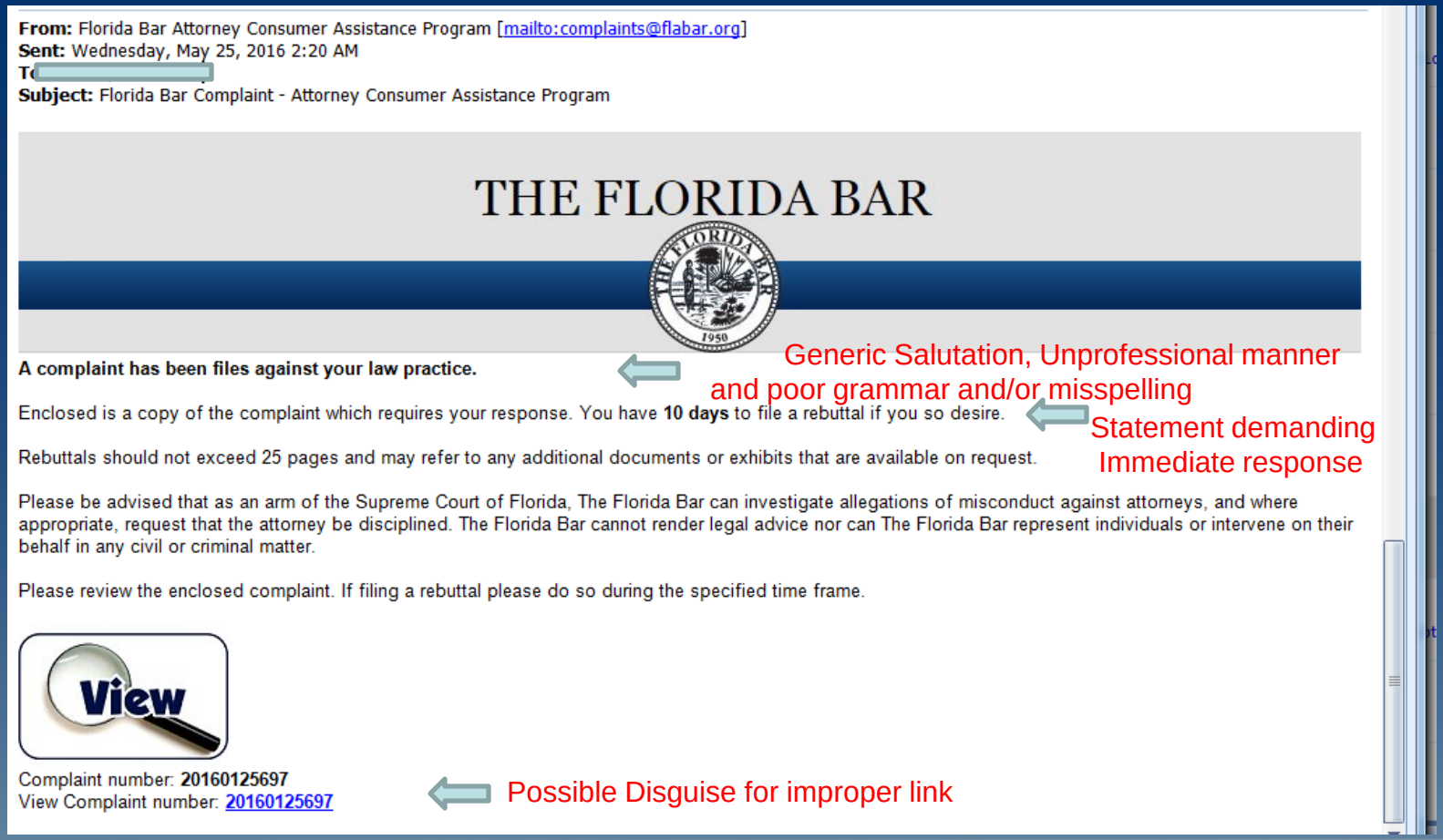
Statistics on Social Engineering Fraud

- Reported Losses of social engineering fraud in 2016 were nearly $1.2 billion.
- FBI has noted that since 2013, losses from phishing have been over $2.3 billion. The financial impact to an organization can be significant.
- 29% of all data breaches in 2013 involved social engineering. In 2016, 95% of those breaches used phishing.
- Certain industries are targeted more than others for fraud

Phishing

- Fraudulently obtaining private information
  - Hacker sending an email that looks like it came from a legitimate business
  - Requesting verification of information and warning of some consequence if not provided
  - Usually contains link to a fraudulent web page that looks legitimate
  - User gives information to the social engineer
    - Ex: Ebay Scam

Phishing (Cont.)



From: Florida Bar Attorney Consumer Assistance Program [mailto:complaints@flabar.org]
Sent: Wednesday, May 25, 2016 2:20 AM
T
Subject: Florida Bar Complaint - Attorney Consumer Assistance Program

THE FLORIDA BAR

A complaint has been files against your law practice.

Generic Salutation, Unprofessional manner and poor grammar and/or misspelling

Enclosed is a copy of the complaint which requires your response. You have **10 days** to file a rebuttal if you so desire.

Statement demanding Immediate response

Rebuttals should not exceed 25 pages and may refer to any additional documents or exhibits that are available on request.

Please be advised that as an arm of the Supreme Court of Florida, The Florida Bar can investigate allegations of misconduct against attorneys, and where appropriate, request that the attorney be disciplined. The Florida Bar cannot render legal advice nor can The Florida Bar represent individuals or intervene on their behalf in any civil or criminal matter.

Please review the enclosed complaint. If filing a rebuttal please do so during the specified time frame.

View

Complaint number: **20160125697**
View Complaint number: 20160125697

Possible Disguise for improper link

Phishing (Cont.)

From: Emily Weissenberger [mailto:emily.weissenberger@gmail.com]
Sent: Monday, February 27, 2017 1:34 PM
Subject: Review the attachment

Hello,

Generic Salutation

Hope this finds you well,

Attached documents has been shared with you using a verified file viewer.

Please find the attached.

Generic Sign-Off

Kind regards

Message | IT Admin Desk.pdf (187 KB)

Possible Disguise for attachment

From: William Foutz [mailto:William.Foutz@dayco.com]
Sent: Monday, March 13, 2017 10:25 AM
Subject: IT Admin Desk

This Message is from Help_Desk Administrator. Please read attach message and follow instruction accordingly.

This communication, along with any documents, files or attachments, is intended only for the use of the addressee and may contain confidential or privileged information. If you are not the intended recipient, you are hereby notified that any dissemination, distribution or copying of any information contained in or attached to this communication is strictly prohibited. If you have received this message in error, please notify the sender immediately and destroy the original communication and its attachments without reading, printing, or saving in any manner.

Phishing (Cont.)

- Spear Fishing (Specific Phishing)
  - Ex: email that makes claims using your name
- Vishing - where criminals persuade victims to hand over personal details or transfer money, over the telephone. They have a number of techniques at their disposal.
- “Whale phishing” or “whaling” is spear phishing but for bigger fish — in other words, CEOs, CFOs and other senior executives with the power to authorize major money transfers or release sensitive data.

Mobile/Home Devices Under Attack

- Smishing - hackers using texts to smart phone to send malware
- Malware infects device & exposes work data
- Phones/home devices not protected with firm anti-malware
- Less security or no security - used by others
- Work documents sent to home

Ransomware

Malware from advertisement on internet or email attachment

Firm's antivirus blocks it from infecting the firm network

All data and shared files on the computer already encrypted

Files cannot be unscrambled without paying a hefty fee

IT removes computer from network, but must recreate data

WILSON ELSER

Facts about Ransomware (Computerworld)

- Average ransom increased in 2016 to $1,077 from $294
- 36% increase in attacks in 2016
- Ransom kits cost between $10 and $1800
- Consumers were 69% of targets; business were the rest
- 34% pay the ransom, *only 47% got access to the data*
- 77% of attacks are through email
- 33% involved voluntary divulging of personal information (as opposed to malicious link or attachment)

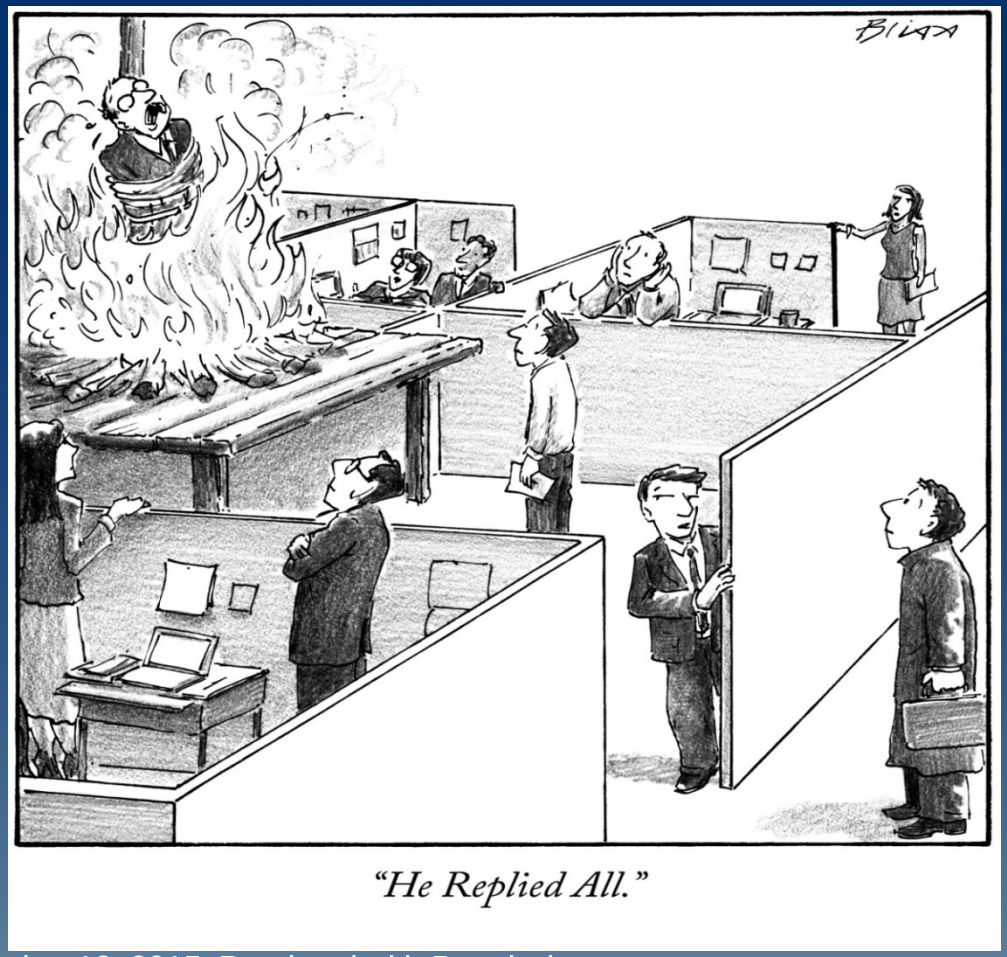
General Background on Other Social Media Exposures

- Pretexting / Impersonation– Creating a fake scenario
- Fake Websites / Cloning– Molded to look like the real thing. Log in with real credentials that are now compromised
- Fake Pop-up – Pops up in front of real web site to obtain user credentials
- Malware-infected software (keystroke viruses)

Lawyers Misuse of Technology

- Public Wifi – easy interception
- Including personal information in public filings
- Password deficiencies (weak and security issues)
- Sloppy or rogue employee
- "Reply to all" mistakes
- Disclosing and reviewing Metadata – ethical issues
- Misuse of mobile devices and home computers

Reply to All



"He Replied All."

From The New Yorker, September 12, 2015, Reprinted with Permission.

Lawyers' Mishandling of Hardware

- Lost devices – work data compromised
- Stolen devices –mobile or home devices
- Improper disposal – home/mobile/work devices
- USBs/external hard drives –portable and not secure
- Cloud computing
- Obsolete hardware & software – subject to easy attack
- Lawyers slow to report
- Physical security in the office

What About Metadata?

- “Drafting Information about information”
  - Dates of creation or access
  - Authors
  - Editing history
  - Management and retrieval information
  - Track changes
- Applies to documents, emails, spreadsheets, PowerPoint presentations and databases

Ethical Issues with Metadata

- Is there a duty to delete metadata before sending a document?
- Can you search for metadata in a document you receive from opposing counsel?
- Do you have to notify the other side if you inadvertently receive a document with metadata?
- Do you have an obligation to produce non-privileged metadata with documents if not requested?
- Can parties affirmatively seek metadata in litigation?

Consequences of a Data Breach

- Cost of issuance of breach notice
- Business interruption
- Media failure - damaged data, damaged hardware & cost of repair
- Additional business overhead
- Injury to business associates
- Reputational injury
- Ransom
- Civil penalties
- Audit of the firm's data security

What Law Firms Should Do: Practical Take Aways for Cyber Risk

- The first line of defense is the best and latest software to filter out as much suspicious activity as possible.
- Risk management awareness and training
- Strict protocols around wire transfers and information
- User Awareness
  - User knows that giving out certain information is bad
  - Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about internal information
  - Do not provide personal information, nor information about the company(such as internal network), unless authority of person is verified

Ways to Avoid a Phish

1. Never click on a link, photo or attachment from anyone you don't know, or involving a transaction you did not make, no matter how harmless it appears or what the attachment purports to be.

2. Never click on a link, photo or attachment you were not expecting to receive, even if you know the sender – call first. Avoid dangerous file types.

3. If you ever open an attachment and are asked to open a zip file, click on a box, enable a new software version, or update or enter information – **STOP**! Close out of the email immediately.

WILSON ELSER

Protecting Against Phishing

1. Hover over “From” Column to better identify the sender
2. Are the URLs legitimate?
3. Incorrect grammar/spelling
4. Plain text/Absence of logos
5. Message body is an image
6. Reputation of country of origin as to scams
7. Request for personal information
8. Suspicious attachments
9. Urgent/Too good to be true
10. Is my email address listed as the "From" address?

Avoiding Email Wire Transfer Scams

- Never change wiring process from email
- Always call person who changes funding
- Carefully compare the email address on the funding change email and prior known real one

Mobile/Home Devices

- Install anti-virus and anti-malware on phones/tablets
- Password protect all devices and wifi
- Enable "find my iPhone" feature
- Firm must require immediate notice of lost device and right to wipe lost device (will include personal data)
- Keep separate devices for work and personal
- Upgrade all the operating systems

Know Your Client

- Meet client face to face! (foreigners too)
- Get ID (passport, driver's license)
- Google/Facebook search
- Ask your firm colleagues
- Check court dockets
- Know source of deal funds & deal purpose

More Practical Take Aways

- Encourage caution & double-checking
  - Before transmitting personal information over the internet, check the connection is secure and check the url is correct
  - If unsure if an email message is legitimate, contact the person or company by another means to verify
- Employ technology-based solutions to filter emails.
- Be paranoid and aware when interacting with others on anything that needs protected

Law Firm Management & Cyber Risks

- Clients expect competency
- The Approach:
  - Treat cyber risk like a business problem.
  - **Systematically** Define, Plan, Execute and Evaluate.
- Methodology:
  - skills, tools, processes.
    - Some already in place.
    - Some will be new.
- Phases of each case:
  1. Scoping & Planning
  2. Execution
  3. Closing

Legal Project Management ("LPM") – An Overview

- Best Practices are Standards – The way we do our work.
  - Steps that we know lead to the best result.
- Areas of Focus:
  - Activities – What work we do
  - Process – How we do our work
  - Timing – When we do our work
- Benefits of Documenting Best Practices:
  - Best results – Repeat what works
  - Avoid mistakes
  - Consistency of work product
  - Teaching tools
  - Sharing information
  - Support planning and budgets
- Have Best Practices include consideration of Cyber Risk.

Identify and understand Stakeholders / Clients

- **Stakeholder: Anyone who can impact (positively or negatively) the handling and outcome of a legal assignment.**
- Why is this important?
  - Gives an understanding of client business/business needs.
  - Allows you to tailor reporting to ensure that true stakeholders are well informed.
  - In litigation, authority is key- knowing who makes decisions, how those decisions are made and when, is valuable information.

Applying Law Firm Management

- Front-load your work. Spend much more time planning the work to understand what tasks are required, how long they will take, who is best suited to do them, and how much it will cost.
  - Avoid fixing problems later (damage control is less valuable than good planning).
  - Plans have to be realistic.
  - Plans should anticipate change.
- Delegate – Use people to their full capability.
- Recognize the benefits:
  - Firm: Financial impact
  - Lawyers: Less time spent on reacting by being proactive.
  - Clients: Safer/Confident with law firm handling the work.

Common Project Management Roles

- Champion
  - High level firm leader with appropriate influence and authority to advance initiatives and drive key decisions.
- Sponsor
  - Business process owner. Relationship or Admin partner level with accountability for client relationships or business processes.
  - Provides key support in securing resources to complete project work.
- Project Manager
  - Oversees and coordinates projects
  - Enforces timetables and deliverables
- Team Members
  - Various levels of attorneys and other professionals familiar with the work at issue and able to take on elements of the project.
- Subject Matter Experts
  - People who provide specific skills and expertise needed for the project.

Law Firm Management

Scoping

- Agree on Expectations
- Scope of Work
- Plan Communication
- High Level Milestones
- Required Resources
- Risks & Assumptions

Planning

- Schedule
- Staffing
- Deadlines & Dependencies
- Change Management Plan
- Budget

We generally combine Scoping & Planning Phases and generate a single project document that serves as the Charter and Project Plan

LPM vs Non-LMP - Scoping

LPM

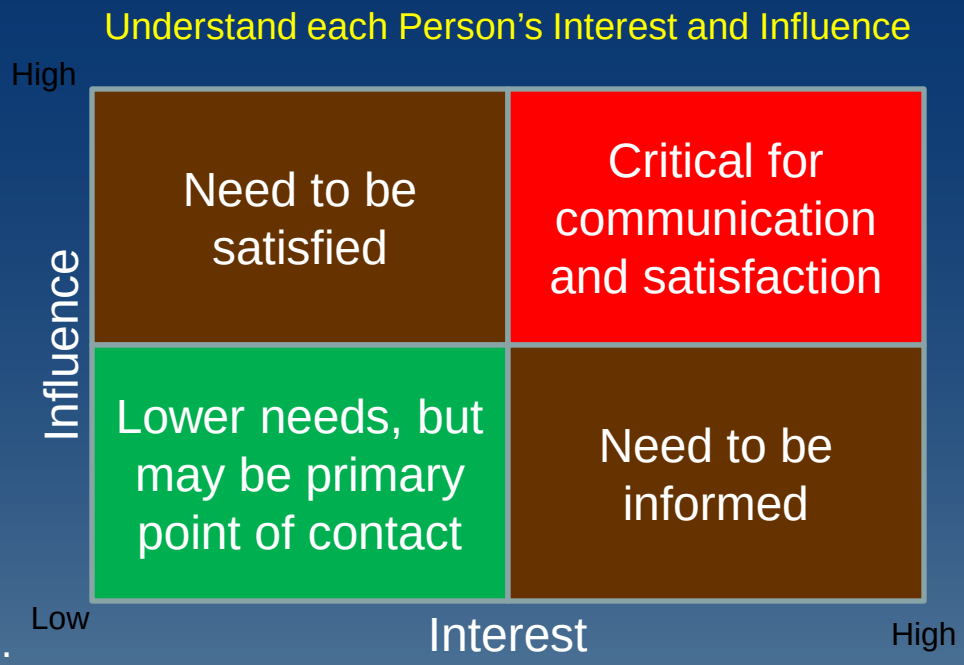
- **Transparency- Predictability** - Discuss the case plan, staffing, anticipated activities and preferred resolution up front, with client and with your team. Upfront discussions about possible variations to plan.
- **Consistency** – case is managed consistent with prior matters – by all offices and team members.
- **Safety/Security** – data is protected by following best practices.

Non-LPM

- Start the work, assign tasks to the team and report outcomes of activities to client.
- Each office or team develops their own approach to case management.
- Attorneys not aware of how to access data safely.

An Example of LPM Scoping Methodology: Stakeholder Analysis

- **Stakeholder: Anyone who can impact (positively or negatively) the handling and outcome of a legal assignment.**
- Identify them to:
  - Set expectations
  - Identify Risks/Concerns
  - Plan communication
- Who are they?
  - Provide information and documents;
  - Receive communication/reports;
  - Determine settlement authority;
  - Authorize strategic decisions;
  - Approve budgets;
  - Pay legal bills or other costs; or
  - Define your "success."
- Share the assessment with your team.
- Reassess – people and roles can change.



Planning and Budgeting

- Plans and Budgets are interrelated concepts.
  - Plans document your expected work, staffing and timeline.
  - Budgets depict your plan financially.
- A useful budget provides a reliable forecast of anticipated legal services and costs.
- Effective budgeting can be a key component of client satisfaction. It fosters confidence in our ability to project and control cost.
- Understand the potential cyber risks on each project:
  - Data gathering
  - Client communications
  - Fund transfers

LPM: Execution Phase

- Doing the Work.
- Managing the Legal Work as Project
  - Handling Changes in Scope – Avoiding Scope Creep
    - Scope can change because of client, opposing counsel, court orders, etc.
    - Discuss & document changes, impact and agreement to modify plan
    - Some firms document via a change control log
  - Managing Stakeholder Communications
    - Review meetings
  - Managing the Project Team
    - Communicate within the team
    - Effective Delegation & Supervision
    - Work charting tools. Project Management tools
  - Monitoring the Budget
    - Manage tasks to the budget
  - Protecting Data
    - Use of encryption or drop boxes with sensitive information

LPM vs Non-LMP - Execution

LPM

- **Transparency - Predictability** – Scope creep is addressed up front. Communications are timely and effective.
- **Consistency** – Budgets are honored or adjusted proactively. Team is consistent and coordinated.

Non-LPM

- Cases competently handled, but scope changes are handled reactively or perhaps not recognized.
- Budgets are not monitored or followed.

LPM: Closing Phase

- Monitor execution to completion
  - Continue to manage the case to conclusion
- Transfer of funds done securely
  - Repeated verification of payment information.
- Lessons learned debrief
  - Engage the client
  - Engage the team
- Capture information and documents that can be re-used
  - Repositories
  - Practice teams
- Close case
  - Final bill
  - Closing papers
  - All buttoned up

Legal Process Improvement (“LPI”)

- Legal Process Improvement: Continuously identifying and implementing ways to make our processes simpler, faster, more efficient and consistent.
- The approach:
  - Client engagement – Voice of the Customer
  - Document Steps in the process
  - Always ask “Why” (Get at the root cause.)
- Future Opportunities:
  - Attorneys or groups who can handle the next case

Legal Process Improvement - Introduction

Common “DMAIC” Approaches:

Lean

- Do the Right Work
  - Adds value
  - Client will pay for it
  - Done right first time
- Simpler, faster, less complex

Six Sigma

- Reduce Variation
- Do the Work Same Each Time
- Consistency & Standardization
- Increase chance of best result

LPM or LPI?

- LPM (Project Management) is helpful to initiate and run discrete projects or assignments.
- LPI (Process Improvement) is helpful to create or refine a process.

➢ The two often work together – a project might include several process improvements.

Process Mapping

- Processes can be “mapped” or visually documented.
- There are different ways to map a process
  - Focus on Activities
  - Focus on Decisions and Work Flow
  - Focus on Handoffs and interaction of people and teams
  - Focus on responsibility of different people
- Process mapping often reveals where we need standards.
  - Inconsistency
  - Critical steps
  - Efficiency

Mapping Processes – The Purpose

- Process mapping creates a visual display of our work.
- Things we learn from seeing a process:
  - Complexity
  - Opportunities to improve efficiency
  - Work that can be done in a different order
- Uses for process mapping:
  - Support case planning and budgets
  - Create training tools
  - Support delegation
  - Support and secure agreement for operational changes
  - Communicate with clients - marketing

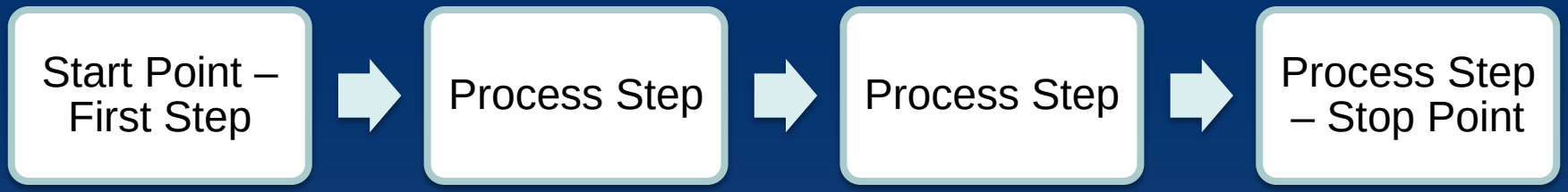
Types of Process Maps

- Different forms of process maps can be used for different purposes.
- There are benefits and limitations to using each kind.
- We will review 4 common types of process maps:
  - Top-Down
  - Logic Flow
  - Swim lanes
  - RACI (“Responsible, Accountable, Consulted, Informed”)

Top-Down Process Mapping - Overview

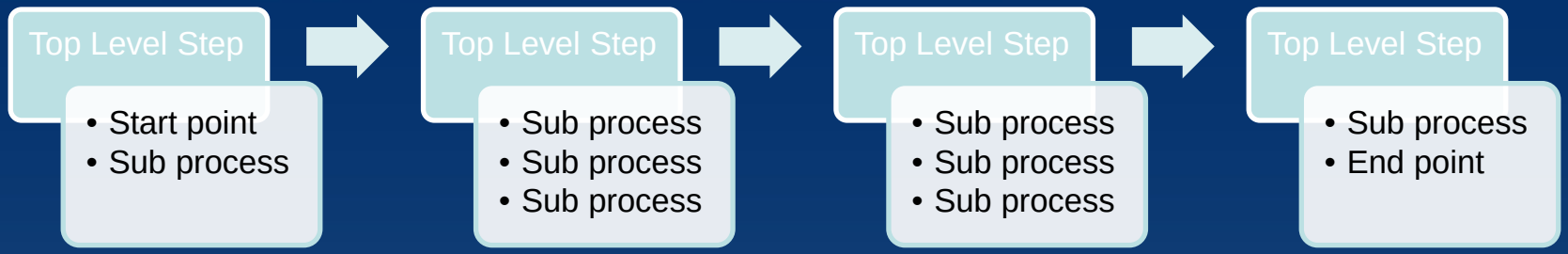
- Simple form of process mapping. Easy to create.
- Common uses:
  - Create checklists
  - Training
- Top Level Steps:
  - Must have a start and stop point
  - Top level is the “what happens”
- Sub-Process:
  - These are the “how’s”
  - Detail covers 80% of the time
  - Identify all the steps that are critical.

Top Level Steps



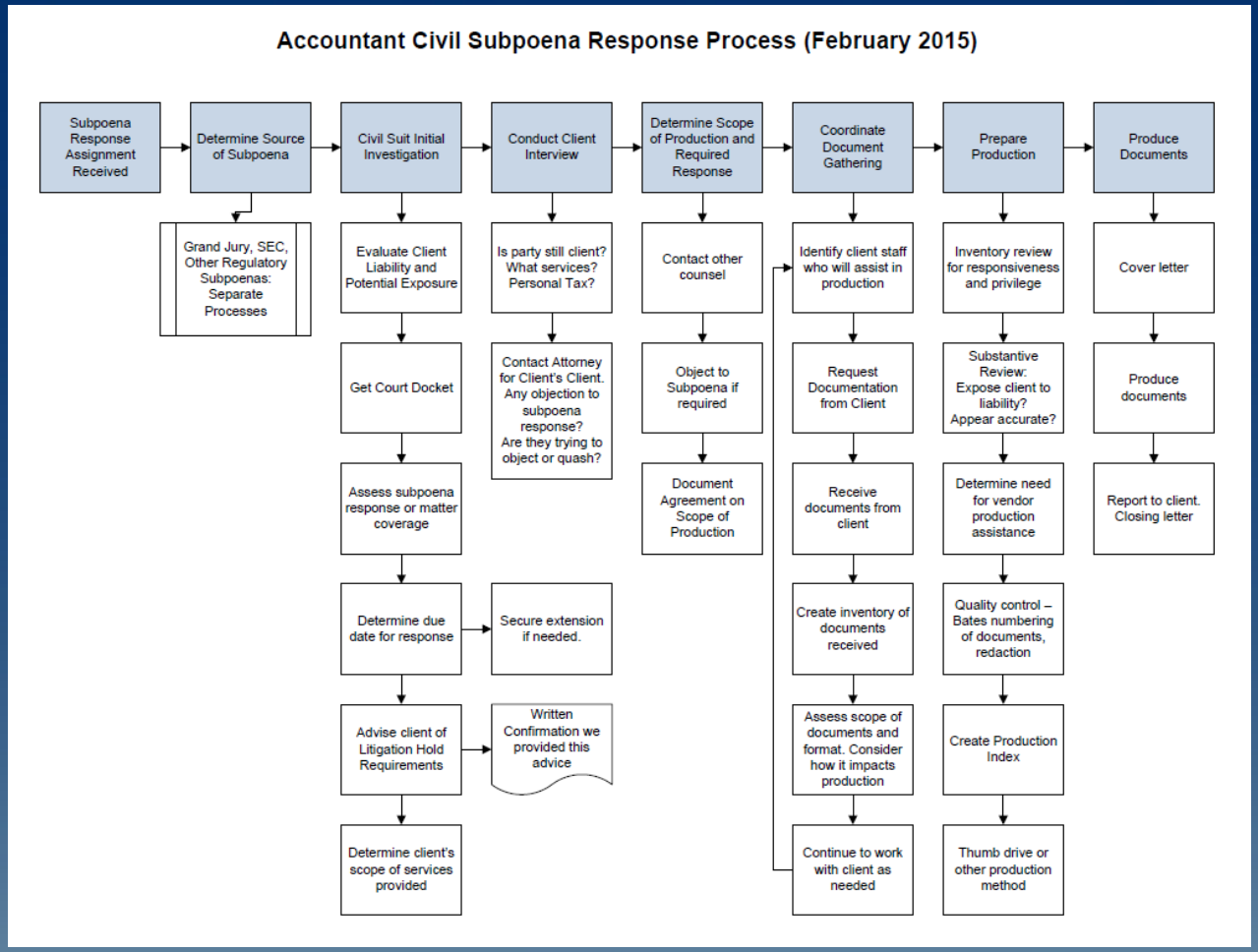
- Top Level is high level

Adding Sub-process



- Sub processes add detail.
- These are the steps that are critical to the Top Level steps.
- Detail:
  - 80% rule. Process map won't cover everything.
  - Consider potential missed steps
  - Consider potential inconsistencies

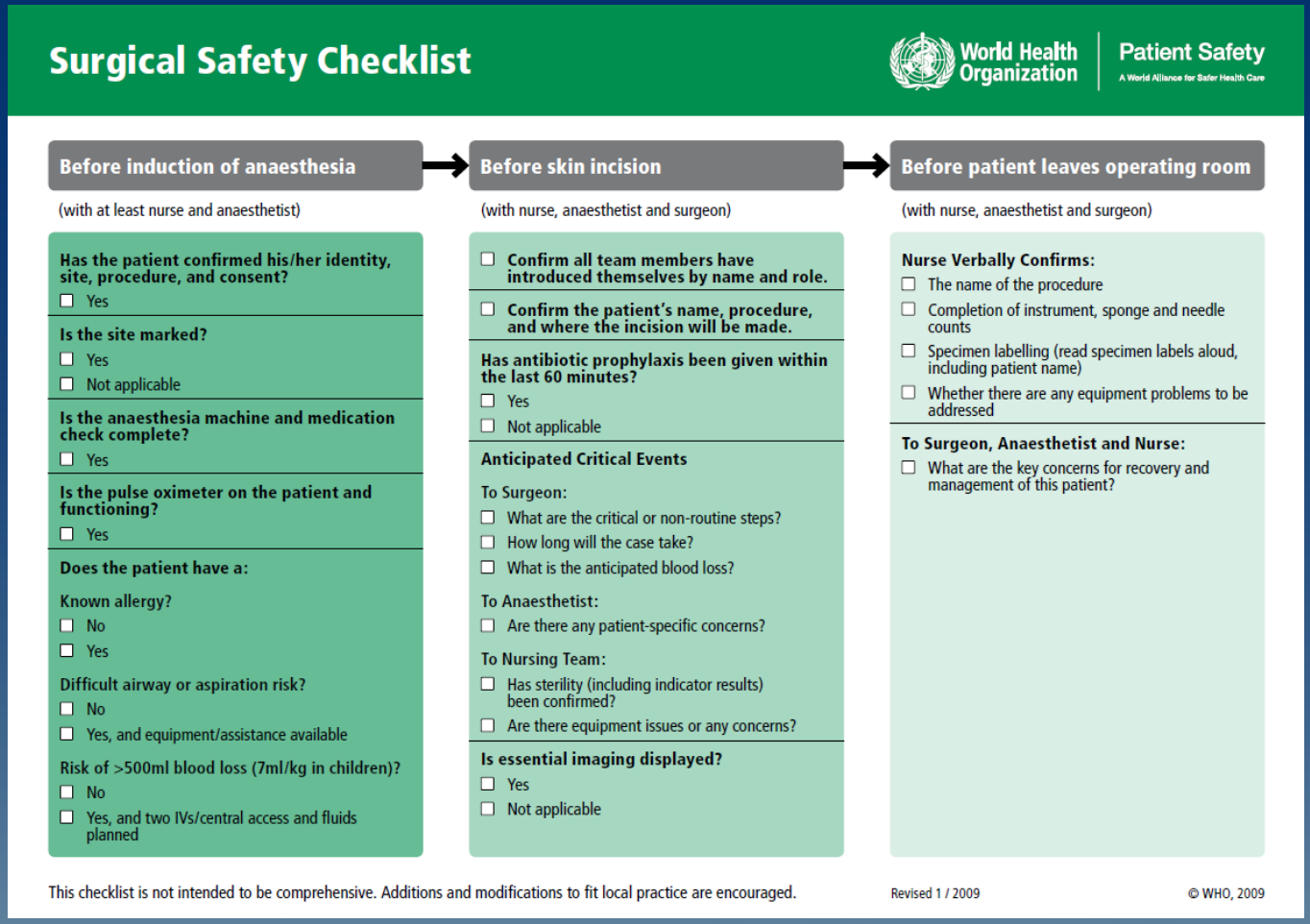
Top-Down Process Map Example



Considerations:

- Does not show work done but not needed.
- Does not show handoffs (who does work).
- Does not show where decisions are made.
- Could have a timeline on top – easy to add.

Creating Checklists



Surgical Safety Checklist

World Health Organization | Patient Safety
A World Alliance for Safer Health Care

Before induction of anaesthesia
(with at least nurse and anaesthetist)

Has the patient confirmed his/her identity, site, procedure, and consent?
- ☐ Yes

Is the site marked?
- ☐ Yes
- ☐ Not applicable

Is the anaesthesia machine and medication check complete?
- ☐ Yes

Is the pulse oximeter on the patient and functioning?
- ☐ Yes

Does the patient have a:

Known allergy?
- ☐ No
- ☐ Yes

Difficult airway or aspiration risk?
- ☐ No
- ☐ Yes, and equipment/assistance available

Risk of >500ml blood loss (7ml/kg in children)?
- ☐ No
- ☐ Yes, and two IVs/central access and fluids planned

Before skin incision
(with nurse, anaesthetist and surgeon)

- ☐ **Confirm all team members have introduced themselves by name and role.**
- ☐ **Confirm the patient's name, procedure, and where the incision will be made.**

Has antibiotic prophylaxis been given within the last 60 minutes?
- ☐ Yes
- ☐ Not applicable

Anticipated Critical Events

To Surgeon:
- ☐ What are the critical or non-routine steps?
- ☐ How long will the case take?
- ☐ What is the anticipated blood loss?

To Anaesthetist:
- ☐ Are there any patient-specific concerns?

To Nursing Team:
- ☐ Has sterility (including indicator results) been confirmed?
- ☐ Are there equipment issues or any concerns?

Is essential imaging displayed?
- ☐ Yes
- ☐ Not applicable

Before patient leaves operating room
(with nurse, anaesthetist and surgeon)

Nurse Verbally Confirms:
- ☐ The name of the procedure
- ☐ Completion of instrument, sponge and needle counts
- ☐ Specimen labelling (read specimen labels aloud, including patient name)
- ☐ Whether there are any equipment problems to be addressed

To Surgeon, Anaesthetist and Nurse:
- ☐ What are the key concerns for recovery and management of this patient?

This checklist is not intended to be comprehensive. Additions and modifications to fit local practice are encouraged.

Revised 1 / 2009

© WHO, 2009

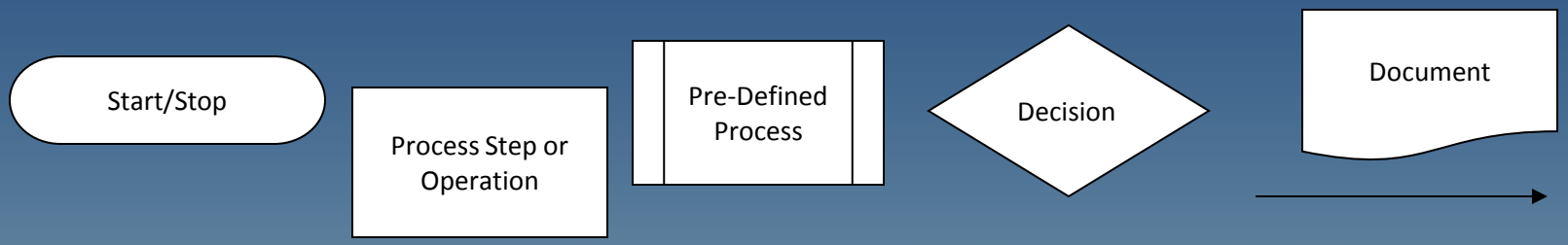
WILSON ELSER

Checklist Tips

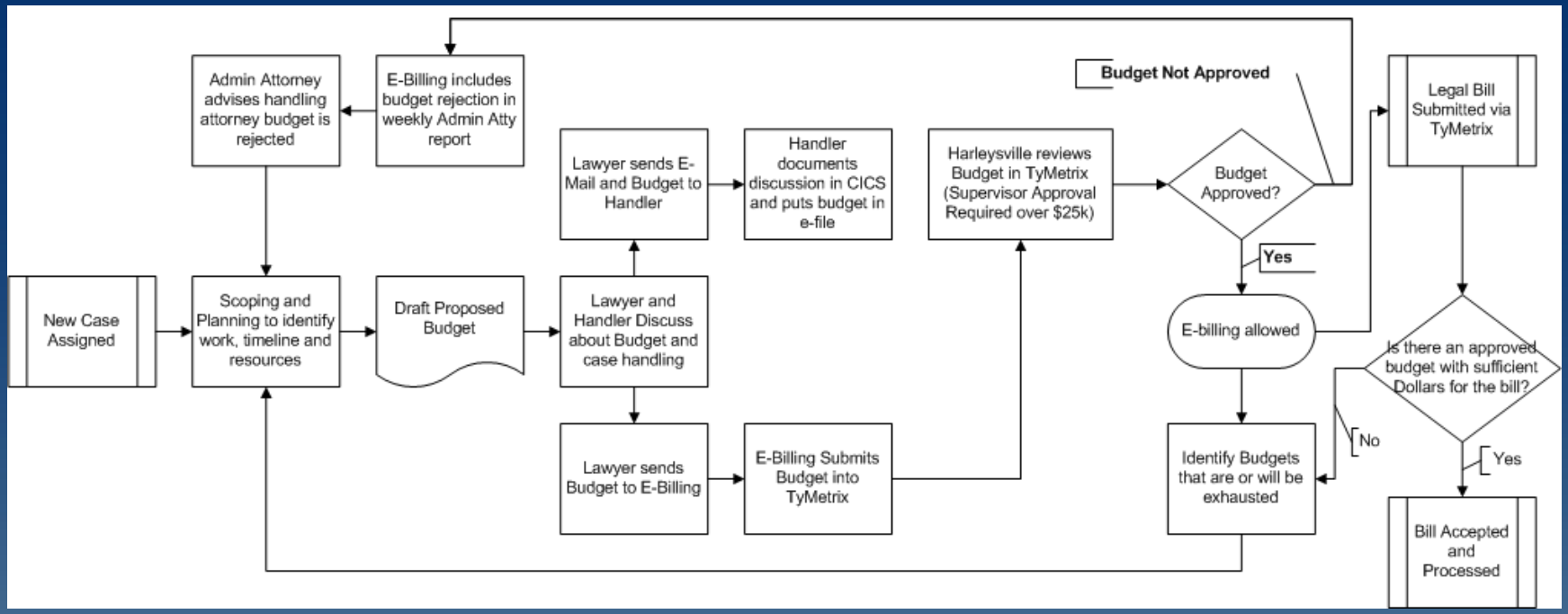
- Fits on a page
- Clear & concise goals
- Critical steps included
- Less than 10 steps
- Each step actionable
- Does it help communication?
- Do you have the right people involved to create?
- Include revision date
- Validate with users

Logic Flow Process Maps

- Flows like we read – left to right.
- Identifies steps that are dependant on something else happening first.
- Shows results of different paths or decisions.
  - Contingencies are useful in creating case plans/budgets & projecting risks
- Can capture a lot of detail. (Can be multiple pages.)
- Still based on activities – does not show who does the work.
- Logical connectors:

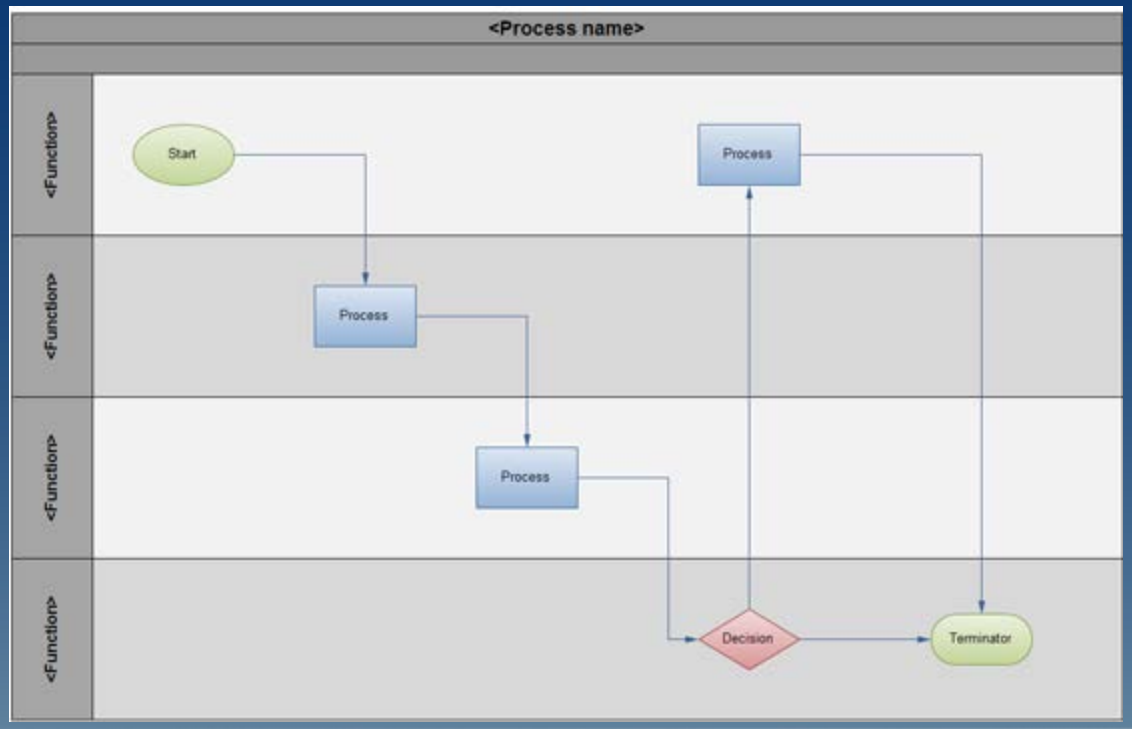


Workflow Example - Budgeting

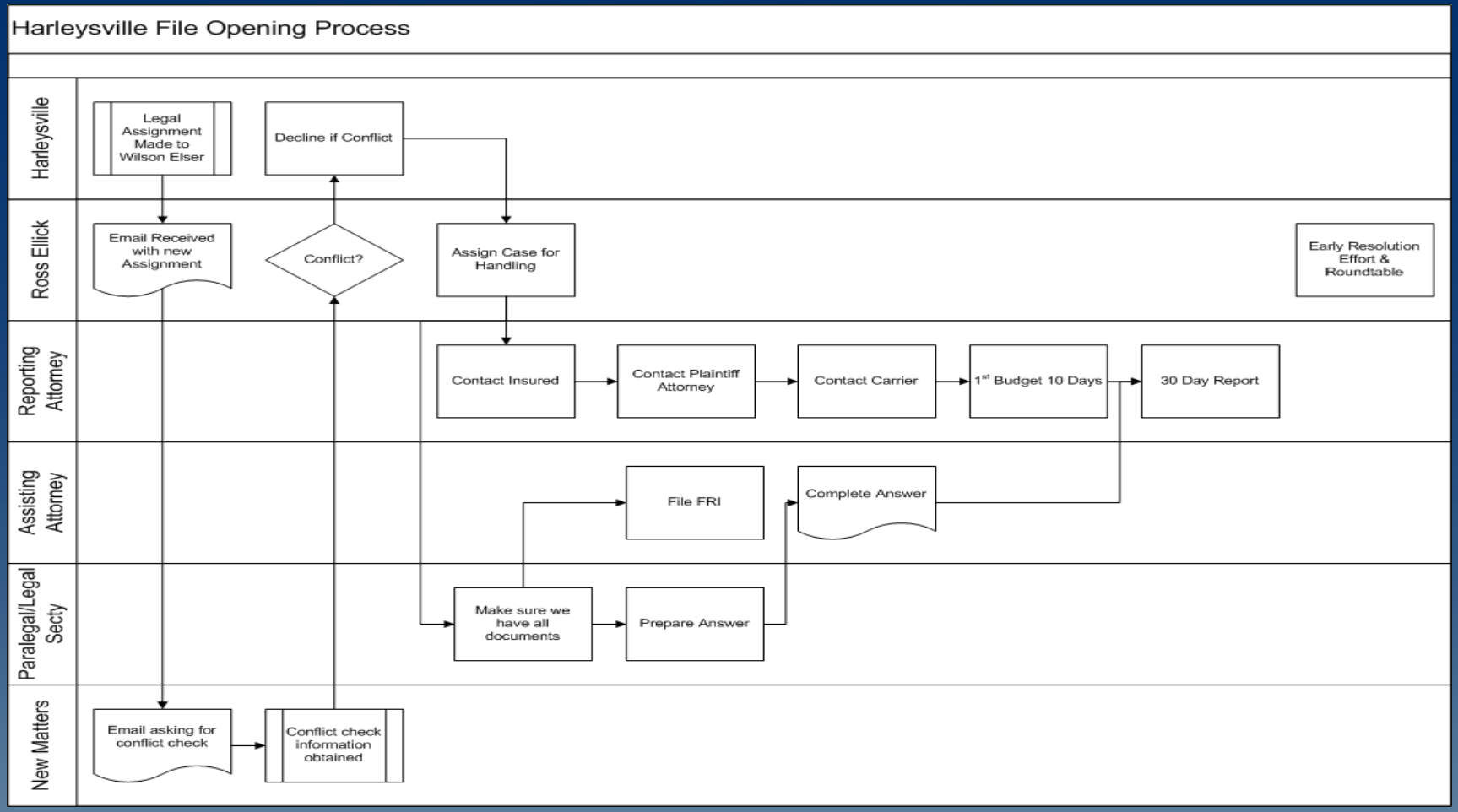


Swim Lane Process Maps

- Harder to create and document.
- Big picture – shows relationship between different people and teams.
- Less about the logical connectors.

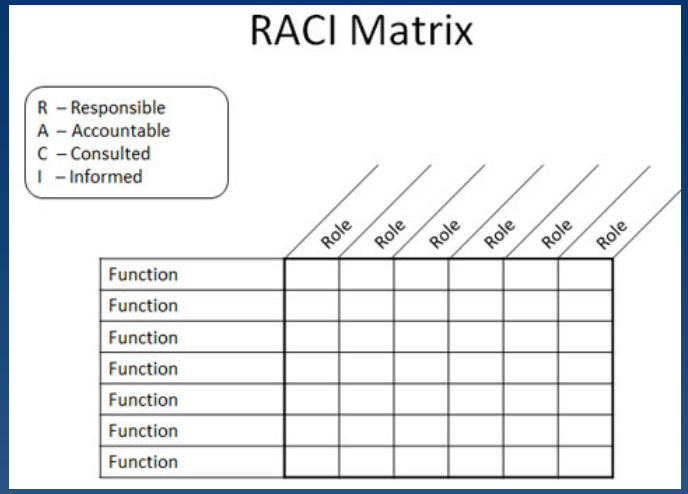


Swim Lane Example – File Opening



RACI Diagrams

- Documents individual roles in a process
- RACI:
  - Responsible
  - Accountable
  - Consulted
  - Informed
- Chart more than diagram
- Use words to describe tasks
- Can show workload issues, bottlenecks and conflicts in roles.
- Budget/Planning tip – are we including time for people who have a role, but are not directly doing the task?

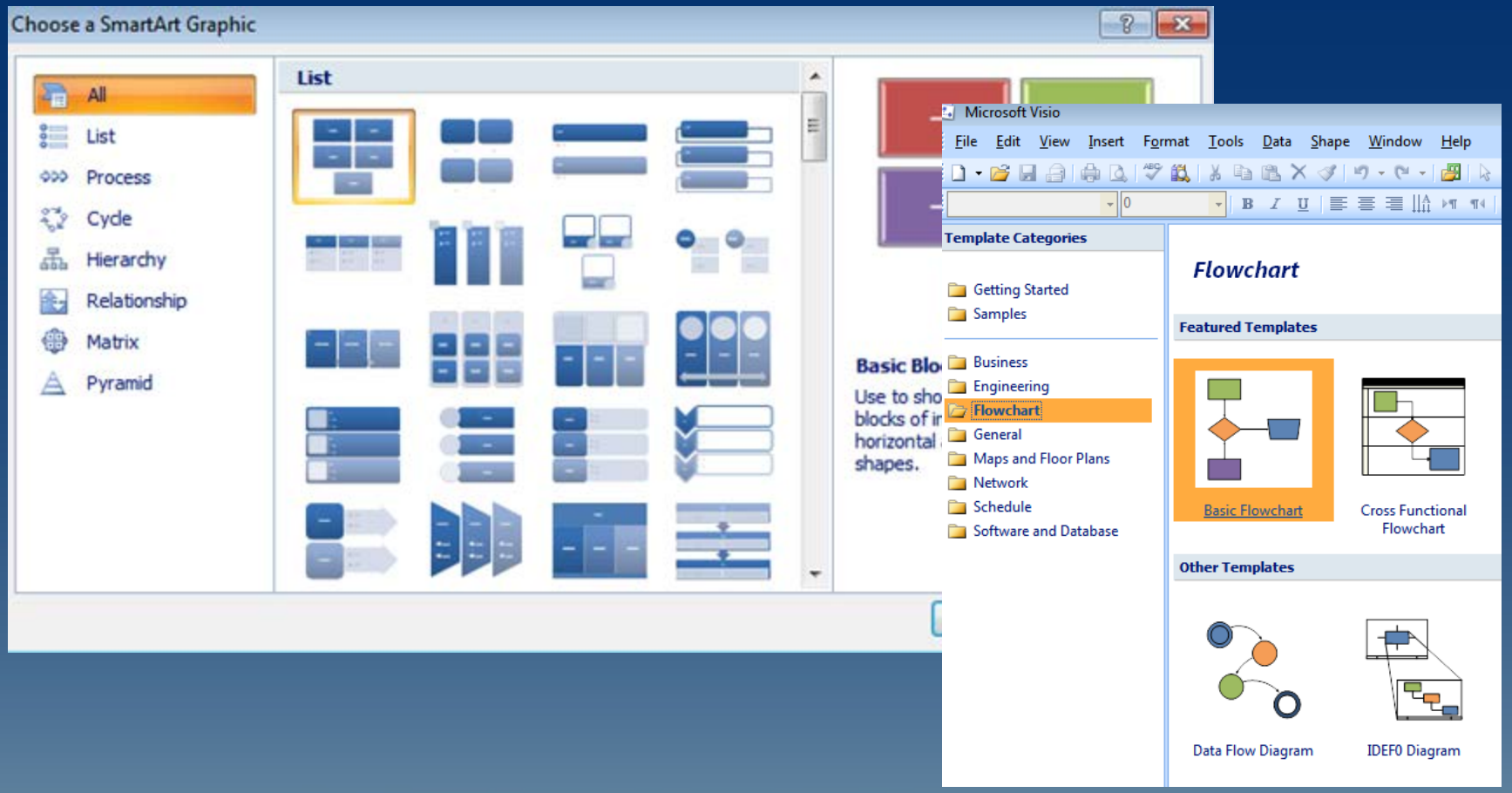


WILSON ELSER

RACI Roles

- **Responsible** - One person performs the work. There must be exactly one person for each task. Every task has to have a person responsible. This is person assigned to the work.
- **Accountable** – Person who has ultimate accountability for the work. This is not needed (or even wanted) in every row. Look for key work and decisions. Only one person can be accountable for any task. Final decision.
- **Consulted** - Person who has to have input before a task is complete or a decision made. There can be multiple people to consult for any task. Consultation has to take place before work or decision.
- **Informed** – Person who has to know about a decision or when work is done. Multiple people can be identified for any task. Information is provided after a decision or action.

Tools to Map Processes



WILSON ELSER

Starting to Process Map

- You can get help. This is a skill that you work to build.
- Identify work that can be mapped.
  - Repeatable series of tasks.
  - Work that can be delegated.
  - Where we want greater consistency.
  - Different people do the work.
- Get the right people in the room.
- Match your process map type to your goals.
- Create Teaching tools, streamline processes, clarify roles, etc.

Contact

Thomas W. Wilson Jr.
Partner
New York, NY
(212) 915-5145
Thomas.WilsonJr@wilsonelser.com

Scott R. Schaffer
Partner
New York, NY
(212) 915-5771
Scott.Schaffer@wilsonelser.com

Jonathan E. Meer
Partner
New York, NY
(212) 915-5639
Jonathan.Meer@wilsonelser.com