Crowe

OneTrust

PRIVACY, SECURITY & TRUST

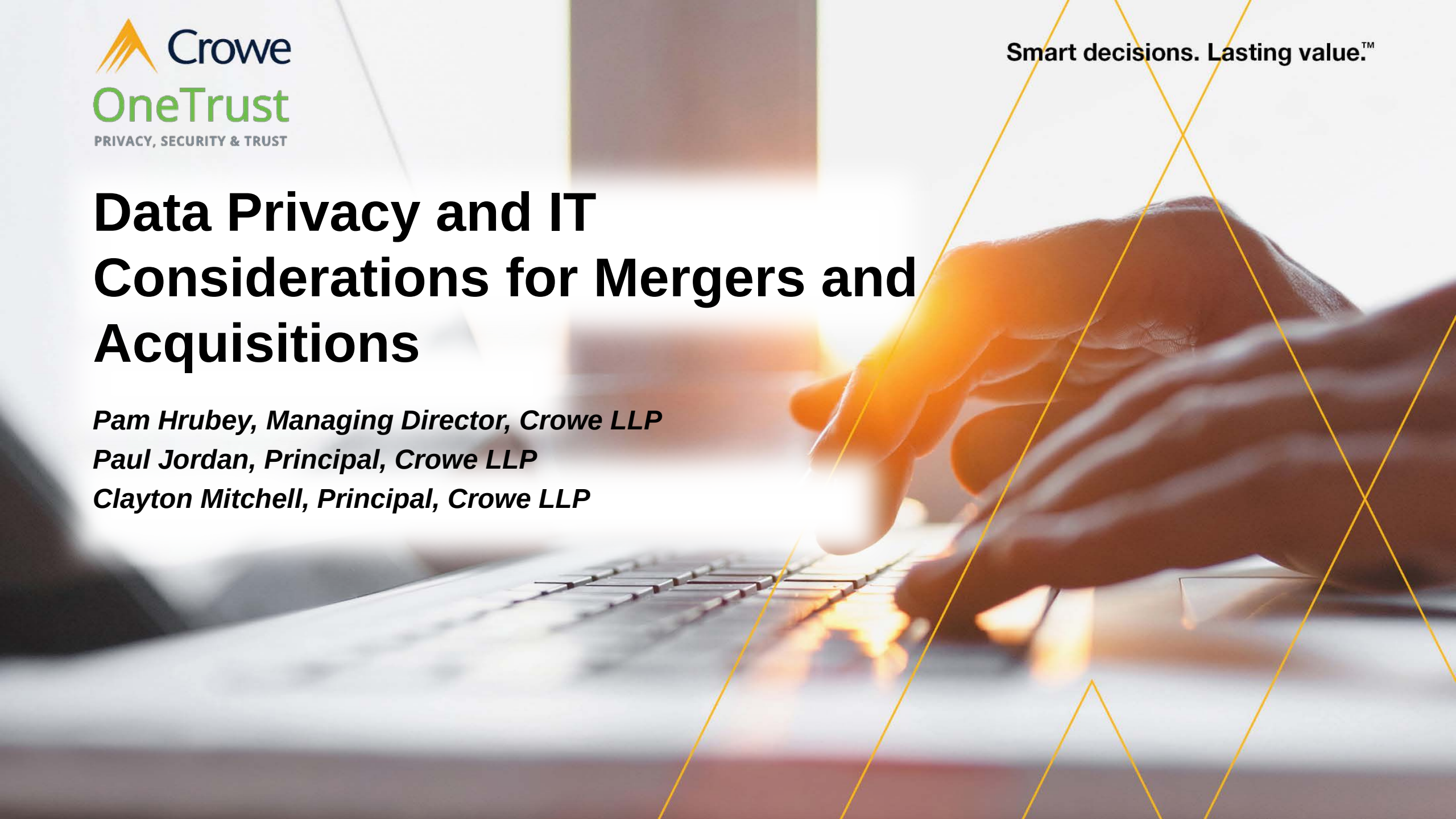
Smart decisions. Lasting value.™

Data Privacy and IT Considerations for Mergers and Acquisitions

Pam Hrubey, Managing Director, Crowe LLP

Paul Jordan, Principal, Crowe LLP

Clayton Mitchell, Principal, Crowe LLP



Objectives

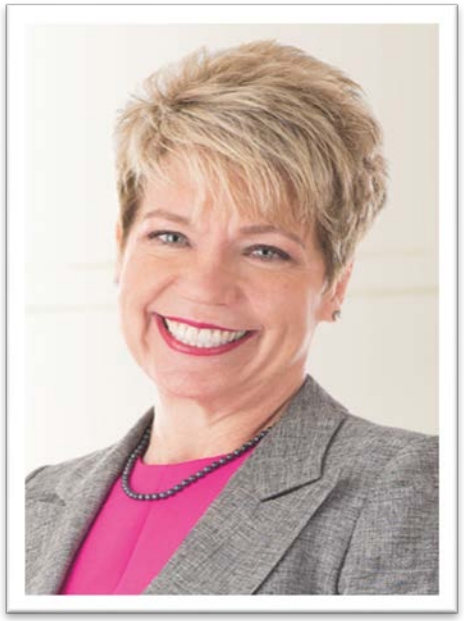
By participating in this webinar, you should be able to:

- Describe the risk or value data can bring to a merger or acquisition
- Outline what questions to ask during the due diligence phase, such as:
  - Was there consent regarding the data collected?
  - Is the information transferable to another company or from one country to another?
  - How can data on clients and customers be used?
- Identify deal-breaking concerns related to poor data management

Agenda

- Using a case study approach…
  - Describe the risk or value data can bring to a merger or acquisition
    - As an acquiring entity, what is the “best case” approach to data-related due diligence?
    - Practically speaking, what usually happens with data-related due diligence?
    - Outline what questions to ask during the due diligence phase, such as:
      - Was there consent regarding the data collected?
      - Is the information transferable to another company or from one country to another?
      - How can data on clients and customers be used?
      - What are the privacy and data protection-related implications for acquiring companies?
  - Identify deal-breaking concerns related to poor data management

Participants in Today's Webinar



Pam Hrubey
Managing Director,
Crowe LLP

Paul Jordan
Principal
Crowe LLP

Clayton Mitchell
Principal
Crowe LLP

Privacy & Data Protection Framework

Crowe Methodology for Privacy & Data Protection Compliance

Accountability & Governance

Determining the organization's risk appetite in relation to data protection, enhancing accountability and governance through policies and standards.

RISK GOVERNANCE
(DP risk appetite and the link to wider Enterprise Risk Management framework)

DATA GOVERNANCE
(ownership, stewardship and control of personal data acquired and processed)

DATA PROTECTION POLICIES & STANDARDS
(enhanced policies and standards to govern the design of operational changes, in line with risk appetite)

Legal, Processes & Organization

Establishing the legal basis for use, the Data Protection Officer/Privacy Officer role, handling data subjects' requests, managing third parties, responding to data breaches, and implementing the supporting organization, process and cultural changes.

CONSENT, USE & LAWFULNESS OF PROCESSING

INDIVIDUAL REQUESTS & RIGHTS
(SAR; RTBF; portability; restriction; rectification)

THIRD-PARTY MANAGEMENT
(legal docs; DD; oversight, 4th parties, supplier network)

BREACH MANAGEMENT & NOTIFICATION

DATA PROTECTION OPERATING MODEL
(DPO/Privacy role; privacy by design; DPIA; line 1 & 2 responsibilities)

TRAINING AND AWARENESS
(delivery of enhanced DP training to meet needs, plus communications and culture change)

Information Security & Data Retention

Understanding and defining the approach to information security and personal data retention.

INFORMATION SECURITY
(electronic and physical)

DATA RETENTION
(deletion; obfuscation; pseudonymisation)

Data Definition, Mapping, & Transfer

Understanding, defining and documenting the personal data that the organization acquires and processes.

DATA DEFINITION & MAPPING
(documenting and classifying uses, locations and internal/external movements of personal data)

CROSS-BORDER DATATRANSFERS
(adequate protections for cross-border transfers)

Stage 1: Strategy

Case Study “Facts”

A global life sciences company, GrowingFast, headquartered in the United States (with operations in North and South America, Europe, the Middle East, and Asia-Pacific region) has grown its portfolio of pharmaceutical products and that has created a new therapeutic area of study. One product in development within this therapeutic area – Diabetes - has been highly effective in clinical trials but requires daily injection. Researchers understand from conducting focus groups that a pen-related device is favored by patients (especially in Asia and in Europe) because of the ease of use and improved safety profile.

After considerable study, GrowingFast researchers realize that designing a pen for daily use would delay the planned 2023 launch of their product by at least a year, making it likely that a competitor would be first to market, removing the current advantage the product would otherwise have. GrowingFast recognizes their product has the potential to address an unmet medical need for Diabetes patients, and so they feel a strong sense of urgency to avoid any unexpected development delays. GrowingFast also recognizes that if a competitor came to market before GrowingFast, the net present value of their innovative product is cut AT LEAST in half. After discussions with senior executives, the decision is made to seek an acquisition of a small device manufacturer who has credibility with regulators.

The company’s business development leaders identify a prime candidate for acquisition. After signing mutual non-disclosure agreements, discussions begin in earnest about the target company’s capabilities.

Information About the Acquisition Target

- The acquisition target, WeMakePenInjectors, has been in business for approximately 25 years. They are headquartered in Ireland, and have manufacturing sites in China, Ireland and the United States. Company leadership resides in the US. WeMakePenInjectors also leverages a network of contract manufacturers to maintain an adequate market supply of their products.

- WeMakePenInjectors has a seasoned leadership team. The CEO hails from the metals industry, and has been at the helm of the company for 10 years. The CFO, COO, and CAE also have a long duration of service to the company. WeMakePenInjectors is privately held, and has annual revenues of $30M US.

- WeMakePenInjectors has 750 employees, including a small team of engineers and a large team of marketeers. WeMakePenInjectors has a very strong web footprint, and leverages a digital marketplace to accept custom order requests from both individuals and companies. They estimate they receive, on average, around 500 design or manufacturing requests a year.

Stage 2: Evaluating & Engaging the Target

WeMakePenInjectors Privacy Efforts

- WeMakePenInjectors does not have a chief information security officer or a privacy officer, but they do have an information security program, and have annual training for US-based employees.

- The company has not engaged in risk assessment-related activities in either the privacy or security space, although the CIO has been pitching the idea to other management team members in light of the potential for acquisition by another entity.

- The company has received several requests for information from employees in Ireland. Those requests were forwarded to human resources and handled as time allowed. The requests seemed to stem from a possible data breach involving a US-based payroll processor. The payroll processor notified WeMakePenInjectors of the possible breach 5 months ago but there has not been any additional communication regarding the situation.

- WeMakePenInjectors was advised by external legal counsel to certify to the EU US Privacy Shield in order to transfer customer, employee, and direct-to-consumer-related advertising metrics to the US.

WeMakePenInjectors Information Technology Efforts

- WeMakePenInjectors has been acquisitive but opts not to integrate the IT area of its addons and therefore has a fragmented set of capabilities and approaches to IT
- The Company lacks a strong, centralized IT leader who is able to set and enforce a unified set of IT policies and best practices
- The Company maintains a patchwork of systems and infrastructure that are not standardized, supporting the business in silos
- The Company allows personal devices on the network but does not require that mobile device management software or issue company security profiles to secure personal devices
- The Company issues laptops to many of its office employees but does not leverage data loss prevention or device encryption software
- WeMakePenInjectors occasionally scans their environment for vulnerabilities quarterly but does not engage third parties to assess external or internal IT security

Privacy - General Considerations

Buy Side Privacy Due Diligence

Highlights alignment with investment thesis

Areas of Focus

Privacy and personal data-related diligence must provide Investors with commercially-focused, pragmatic insight into:

- Where is the business located and what is the geographic footprint?
- Compliance readiness with privacy-related regulatory requirements.
- Vendor management and 3rd party interactions
- Opportunities to enhance value through modest privacy enhancements

Key Considerations

1. Are there any show-stopping gaps or regulatory issues relating to the management of personal data/information?
3. What scale / growth inhibitors does the privacy program present to the company as it regards personal data?
3. What are the priorities of actions and indicative costs to overcome those inhibitors?

Sell Side Privacy Due Diligence

Prepares seller and maximizes value

Privacy and personal data-related diligence must provide findings & recommendations that:

- Layout a privacy strategy roadmap to show strong data protection'
- Highlight technology capabilities that provide competitive advantages
- Reveal security gaps that should be addressed prior to sale
- Provide quick wins that increase value with a low level of investment

1. What do a sophisticated buyers expect a healthy privacy portfolio to look like?
2. How much should we invest and how do we know if we've overbuilt?
3. Is there a level of technical debt we should retain and what does that look like?

IT Due Diligence – General Considerations

What do IT diligences review at Targets?

Buy Side IT Due Diligence

Highlights alignment with investment thesis

Areas of Focus

Information technology diligence must provide Investors with commercially-focused, pragmatic insight into:

- Strengths and weaknesses of the tech portfolio in a business context; key software, security, infrastructure, user devices, staff and policies
- Compliance readiness with CCPA, GDPR, HIPAA, PCI, CAN-SPAM, etc.
- Vendor management and 3rd party interactions
- Opportunities to enhance value through modest IT improvements

Key Considerations

1. Are there any show-stopping issues that misalign with the investment thesis?
3. What scale / growth inhibitors does the IT organization present to the company in the context of platform?
4. What are the priorities of actions and indicative costs to overcome those inhibitors?

Sell Side IT Due Diligence

Prepares seller and maximizes value

Information technology diligence must provide findings & recommendations that:

- Layout an IT strategy roadmap to show IT strength
- Highlight technology capabilities that provide competitive advantages
- Reveal security gaps that should be addressed prior to sale
- Provide quick wins that increase value with a low level of investment

1. What do a sophisticated buyers expect a healthy IT portfolio to look like?
2. How much should we invest and how does we know if we've overbuilt?
3. Is there a level of technical debt we should retain and what does that look like?

Privacy & Data Protection Framework

Crowe Methodology for Privacy & Data Protection Compliance

Accountability & Governance

Determining the organization's risk appetite in relation to data protection, enhancing accountability and governance through policies and standards.

RISK GOVERNANCE
(DP risk appetite and the link to wider Enterprise Risk Management framework)

DATA GOVERNANCE
(ownership, stewardship and control of personal data acquired and processed)

DATA PROTECTION POLICIES & STANDARDS
(enhanced policies and standards to govern the design of operational changes, in line with risk appetite)

Legal, Processes & Organization

Establishing the legal basis for use, the Data Protection Officer/Privacy Officer role, handling data subjects' requests, managing third parties, responding to data breaches, and implementing the supporting organization, process and cultural changes.

CONSENT, USE & LAWFULNESS OF PROCESSING

INDIVIDUAL REQUESTS & RIGHTS
(SAR; RTBF; portability; restriction; rectification)

THIRD-PARTY MANAGEMENT
(legal docs; DD; oversight, 4th parties, supplier network)

BREACH MANAGEMENT & NOTIFICATION

DATA PROTECTION OPERATING MODEL
(DPO/Privacy role; privacy by design; DPIA; line 1 & 2 responsibilities)

TRAINING AND AWARENESS
(delivery of enhanced DP training to meet needs, plus communications and culture change)

Information Security & Data Retention

Understanding and defining the approach to information security and personal data retention.

INFORMATION SECURITY
(electronic and physical)

DATA RETENTION
(deletion; obfuscation; pseudonymisation)

Data Definition, Mapping, & Transfer

Understanding, defining and documenting the personal data that the organization acquires and processes.

DATA DEFINITION & MAPPING
(documenting and classifying uses, locations and internal/external movements of personal data)

CROSS-BORDER DATATRANSFERS
(adequate protections for cross-border transfers)

Early warning signs and pitfalls

Warning Signs and Pitfalls	Information Technology	Privacy
Accountability and Governance	▪ Weak or no IT leadership ▪ No formal, written policies and lack or demonstrable enforcement ▪ Lack of alignment to business strategy ▪ Under investment in critical areas of IT	▪ Weak or no privacy leadership ▪ No formal, written policies and lack or demonstrable enforcement ▪ Lack of alignment to business strategy ▪ Under investment in privacy and data protection
Legal, Processes & Organization	▪ No dedicated IT function; whether staff or lack of an IT Managed Service Provider (MSP) ▪ No executed Intellectual Property (IP) Rights Assignment Agreements in place ▪ Hardware/Software acquired from eBay ▪ No structured approach to serving the business	▪ No privacy function or data protection officer ▪ No functioning privacy policies and procedures ▪ No program for provisioning data subject rights ▪ No process for legitimate collection of personal data from data subjects ▪ No structured approach to serving the business
Information Security & Data Retention	▪ Nonexistent or weak approach to conducting security reviews and penetration tests ▪ Personal devices allowed on the corporate network without a way to manage them ▪ IT personnel “safeguarding” company data at home	▪ Nonexistent or weak approach to breach detection or prevention ▪ Nonexistent or weak processes for notifying regulators in the event of a possible breach ▪ Data is never destroyed and is used without regard to accuracy
Data Definition, Mapping & Transfer	▪ Sensitive data received over fax, email, phone and written down on paper and left out in the open ▪ Files with sensitive information sent and received over unsecure email	▪ Most staff are unfamiliar with personal and sensitive personal data concepts ▪ No records of processing or data maps, meaning no knowledge of where personal data exists ▪ No documented legal basis for data transfer

Stage 3: Negotiation of the Initial Agreement

Case study details of the negotiation phase

- GrowingFast reaches out to WeMakePenInjectors to test interest in having discussions that could be of “mutual interest”.

- WeMakePenInjectors – after some initial hesitation – agrees to put a mutual non-disclosure agreement in place so that some initial discussions can occur safely for both parties.

- Discussions then begin – at first between the research teams at both organizations, and then with legal and operations-related leaders.

Initial Negotiations

- Researchers discuss the importance of having an injector that is connected to the cloud so that patients and their prescribing physicians can stay connected regarding important health-related indicators.

- WeMakePenInjectors report that they have a connected device in late stage development, and they express interest in learning more about GrowingFast's products.

- WeMakePenInjectors – after learning about GrowingFast's new diabetes product – is very interested in having more detailed discussions as the product seems to be a perfect for their cloud-connected device.

Early warning signs and pitfalls

Warning Signs and Pitfalls	Information Technology	Privacy
Accountability and Governance	▪ Weak or nonexistent IT Strategy that outlines their approach to Cloud ▪ No prior success or undertaking a significant strategic IT initiative	▪ Weak or nonexistent strategy for protecting personal data and processing personal data consistent with privacy notice and consent
Legal, Processes & Organization	▪ Use of 3rd party or open source components supporting the IP with no formality around license review ▪ .	▪ Significant use of third and fourth parties without initial due diligence, supplier standards regarding protection of personal data and ongoing quality program
Information Security & Data Retention	▪ No 3rd party use for security reviews and penetration tests ▪ .	▪ No requirement for third and fourth parties to safely destroy personal data after completing WeMakePenInjector-related tasks.
Data Definition, Mapping & Transfer	▪ .	▪ .Inaccurate or nonexistent map of how personal data moves from WeMakePenInjectors to third and fourth parties

Stage 4: Due Diligence

Case study details of the due diligence phase

- GrowingFast is thrilled to hear that WeMakePenInjectors has exactly the medical device they feel is needed to support registration and marketing of their new pharmaceutical product.
- GrowingFast requests the opportunity to evaluate WeMakePenInjectors as an acquisition target.
- WeMakePenInjectors wants to talk money…they have private investors involved in their business, and they know these investors will expect a significant return on their investments.
- After intense negotiations, it is determined that limited diligence should be conducted pre-letter of intent to get the buyer comfortable with the price the seller is asking for
- New legal documents are put in place that indicate due diligence pursuant to a potential acquisition is planned, and both parties sign.

Privacy Due-Diligence

- Evaluation of the use and flow of personal information
- Evaluation of the amount and type of PI
- Evaluation of out-of-compliance PI (beyond retention period, not properly noticed, or no ‘legal-basis’)
- Evaluation of storage type, methods, and security
- Evaluation of privacy controls
- Evaluation of prior privacy incidents or breaches

- Example: TripAdvisor acquisition of Viator – 5% stock decline after breach became public (ways to avoid future risk and past liability)

IT Due Diligence – High-Level Security Considerations

What are some common security risks we tend to see at Targets?

Software
- Core business systems / external facing web presence
- Mobile device management (MDM)
- Data loss prevention (DLP)
- Device encryption

Hardware
- Firewall & its associated rules / modules / configurations, firmware updates
- IDS/IPS & its associated rules / modules / configurations, firmware updates
- Spam Filters & its associated rules / modules / configurations, firmware updates
- Web Filters & its associated rules / modules / configurations, firmware updates
- Virtual Private Networking (VPN)

Personnel / Vendors
- IT Leadership
- Security awareness training
- Approach to social engineering
- Lack of vendor engagement for cyber security

Governance/Security
- General IT Security policies
- Role based security configuration; principle of least privileges
- Password policies
- Patch Management
- Change Management
- Refresh strategy
- Employee Offboarding process
- Access controls (internal/3rd party)
- Active Directory best practices
- Actionable back-up and recovery process

Intellectual Property
- How access to source code is controlled
- License status of commercial components used in development of the connected product
- Use of open source components and how they are licensed

Data in Target's Possession

IT Due Diligence – Common Data Considerations

What kinds of data could the Target have that possibly heighten risk?

Common Data in Target's Possession

HR data	Highly Sensitive
Payroll data	Highly Sensitive
Compliance data (HIPAA, PCI, GDPR, CCPA)	Highly Sensitive
Customer data	Competitive Sensitivity
Supplier data	Competitive Sensitivity
Operational data	Competitive Sensitivity
Financial data	Competitive Sensitivity
Big data	Competitive Sensitivity

So What Do These Companies Decide To Do?

Sell Side – Privacy Risks

What can sellers do to secure the environment and show strength to buyers?

Risk, Exposure

- Install strong privacy leadership
- Craft a strong integration plan
- Work in constant collaboration with IT leaders
- Adopt best practices in governance, security, procurement and vendor management
- Aggressively adopt a robust privacy policy and related procedures, including those that address provisioning privacy rights for data subjects
- Craft a long-term Privacy Strategy Roadmap aligned to the business strategy – recognizing that the regulatory environment as it regards protecting personal data is in constant flux
- Routinely assess the performance of third and fourth parties handling personal data on behalf of the organization
- Conduct privacy and data protection awareness training for all employees

Opportunity

- Show buyer that privacy has a long-term strategy to support their investment thesis
- Show buyers strength by demonstrating personal data is protected as a strategic asset on loan from the data subject
- Show buyers strength by demonstrating privacy program has adopted best practices in critical areas that tend to inhibit growth, especially those involving blatant misuse of personal data or unmitigated data breaches
- Show buyers that the right privacy and data protection program investments have been made and that the program enhances the strength of the company's products
- Show buyers that the privacy program is proactive in securing personal and sensitive data
- Show buyer transparency by showing results of self-conducted due diligence

Sell Side – IT Security Risks

What can sellers do to secure the environment and show strength to buyers?

Risk, Exposure

- Install strong IT leadership
- Craft a strong integration plan
- Retain an IT MSP to stand-up a baseline level or IT
- Adopt best practices in governance, security, procurement and vendor management
- Aggressively adopt an IT Shared Service model
- Craft a long-term IT Strategy Roadmap aligned to the business strategy
- Routinely leverage 3rd parties to assess the security posture
- Conduct security awareness training for all employees

Opportunity

- Show buyer that IT has a long-term plan to support their investment thesis
- Show buyers strength by demonstrating IT is a strategic enabler
- Show buyers strength by demonstrating IT has adopted best practices to critical areas that tend to inhibit growth, including security
- Show buyers that the right IT investments have been made and that IT has little to no technical debt, risk, and exposure
- Show buyers that IT is proactive in securing sensitive and competitive information
- Show buyer transparency by showing results of self-conducted due diligence

So How Does This Story End?

- After processing the results of the IT and privacy program due diligence, while GrowingFast continues to be enamored with WeMakePenInjectors' connected device, they are disappointed by the significant gaps they identified during due diligence. GrowingFast lowered the valuation of WeMakePenInjectors.
- WeMakePenInjectors recognized the business opportunity they have for bolstering their internal and external privacy and security-related programs. Because they felt they were in a good position to quickly remediate their gaps, and because their leaders more fully realize the potential value of WeMakePenInjectors' products, WeMakePenInjectors walks away from talks with GrowingFast.
- They resolve to take the following actions:
  - Make additional investments in IT and privacy-related governance, policies and procedures, and technical processes and programs
  - Recruit and hire IT and privacy program leaders to institutionalize new programmatic and technical changes

Thank You

Pam Hrubey
Managing Director, Crowe LLP
Indianapolis, IN
pam.hrubey@crowe.com

Paul Jordan
Principal, Crowe LLP
South Bend, IN
paul.jordan@crowe.com

Clayton Mitchell
Principal, Crowe LLP
Indianapolis, IN
clayton.mitchell@crowe.com