Protecting your next investment: The importance of technology due diligence

August 20, 2019

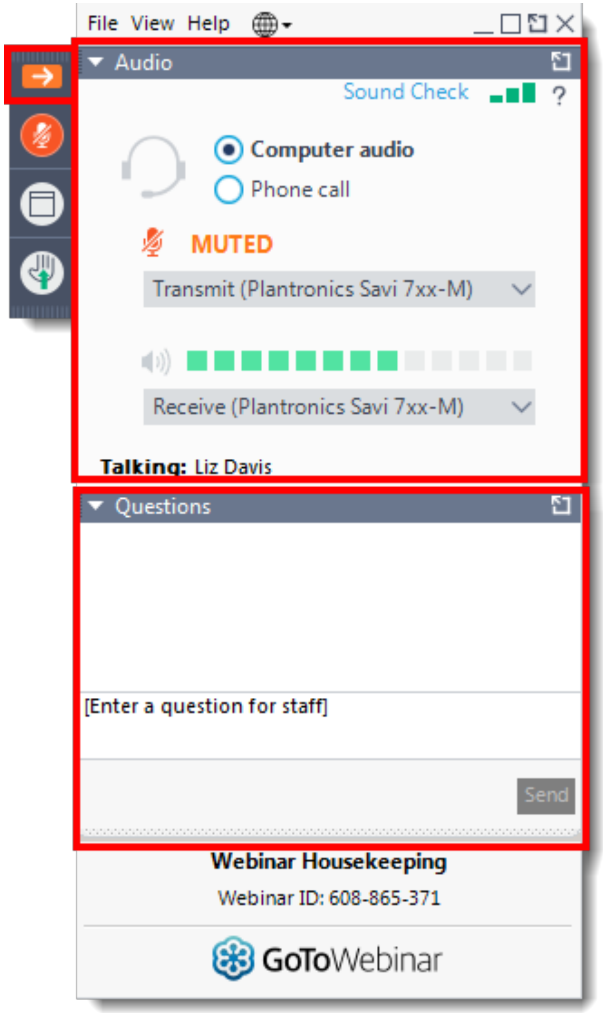
bakertilly

now, for tomorrow.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought. Tax information, if any, contained in this communication was not intended or written to be used by any person for the purpose of avoiding penalties, nor should such information be construed as an opinion upon which any person may rely. The intended recipients of this communication and any attachments are not subject to any limitation on the disclosure of the tax treatment or tax structure of any transaction or matter that is the subject of this communication and any attachments. Baker Tilly Virchow Krause, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities.

GoToWebinar use

- **Everyone is muted to avoid background noise.** Please use the Q&A panel if you need to communicate with the host.
- **Asking questions:** In the Q&A panel, ask questions by choosing “All Panelists” in “Send to” field. Type your message in the Q&A panel and hit “send.”
- **If disconnected:** Refer to your email and reconnect. If audio is disconnected, click on the Communicate menu in the upper left to find the dial in numbers and access code or refer back to your email for the dial in #.
- **Support #:** If you have any technical problems, call GoToWebinar support at 1-877-582-7011
- **We will be recording today’s presentation.**



● Computer audio
○ Phone call

MUTED

Transmit (Plantronics Savi 7xx-M)

Receive (Plantronics Savi 7xx-M)

Talking: Liz Davis

[Enter a question for staff]

Webinar Housekeeping

Webinar ID: 608-865-371

GoToWebinar

bakertilly
now, for tomorrow.

Continuing professional education credit

- This webinar qualifies for 1 hour of Continuing Professional Education (CPE)
- To qualify for the CPE credit, you must be in attendance for the entire webinar, participate in polls and complete the evaluation form at the end of the webinar
- Qualified attendees will receive CPE certificate in 4-6 weeks
- Questions regarding the CPE for this webinar can be sent to Hannah.Brylow@bakertilly.com

Baker Tilly Virchow Krause, LLP is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.learningmarket.org.

Presenters

Bill Chapman
Partner
Transaction advisory services

Atit Shah
Partner
Risk, internal audit and cybersecurity

Brian Nichols
Director
Risk, internal audit and cybersecurity

Agenda

- Risk profile and the growing need for technology due diligence
- What is a technology due diligence assessment?
- Case studies
- Managing IT and cyber risks post-acquisition
- Q & A
- Additional services and resources

Risk profile and the growing need for technology due diligence

Risk profile

Alpha is the risk that a prudent investor expects to be compensated for beyond the risk associated with the market at large.

This unsystematic risk is often referred to as the risk profile of the target company, and it leads to important questions:

1. What should we be looking for?
2. Which techniques can we use to identify the alpha within a target company that will help the investor assess the appropriate price and structure of a particular transaction?

Growing need for technology due diligence

93%

view cybersecurity evaluations as important to their company's M&A decision-making

73%

said uncovering a previously undisclosed data breach during the M&A process would be an "immediate deal breaker"

#2

ranking of "cybersecurity incidents" on the list of most important factors when performing due diligence

81%

are more concerned about a target's cybersecurity practices than they had been in the past

65%

said unforeseen cybersecurity issues had caused their companies to have buyer's remorse in the wake of an acquisition

Source: https://www.mayerbrown.com/en/news/2019/06/cybersecurity-concerns-becoming-a-bigger-part-of-ma-due-diligence-survey-shows

Impacts of cyber crime

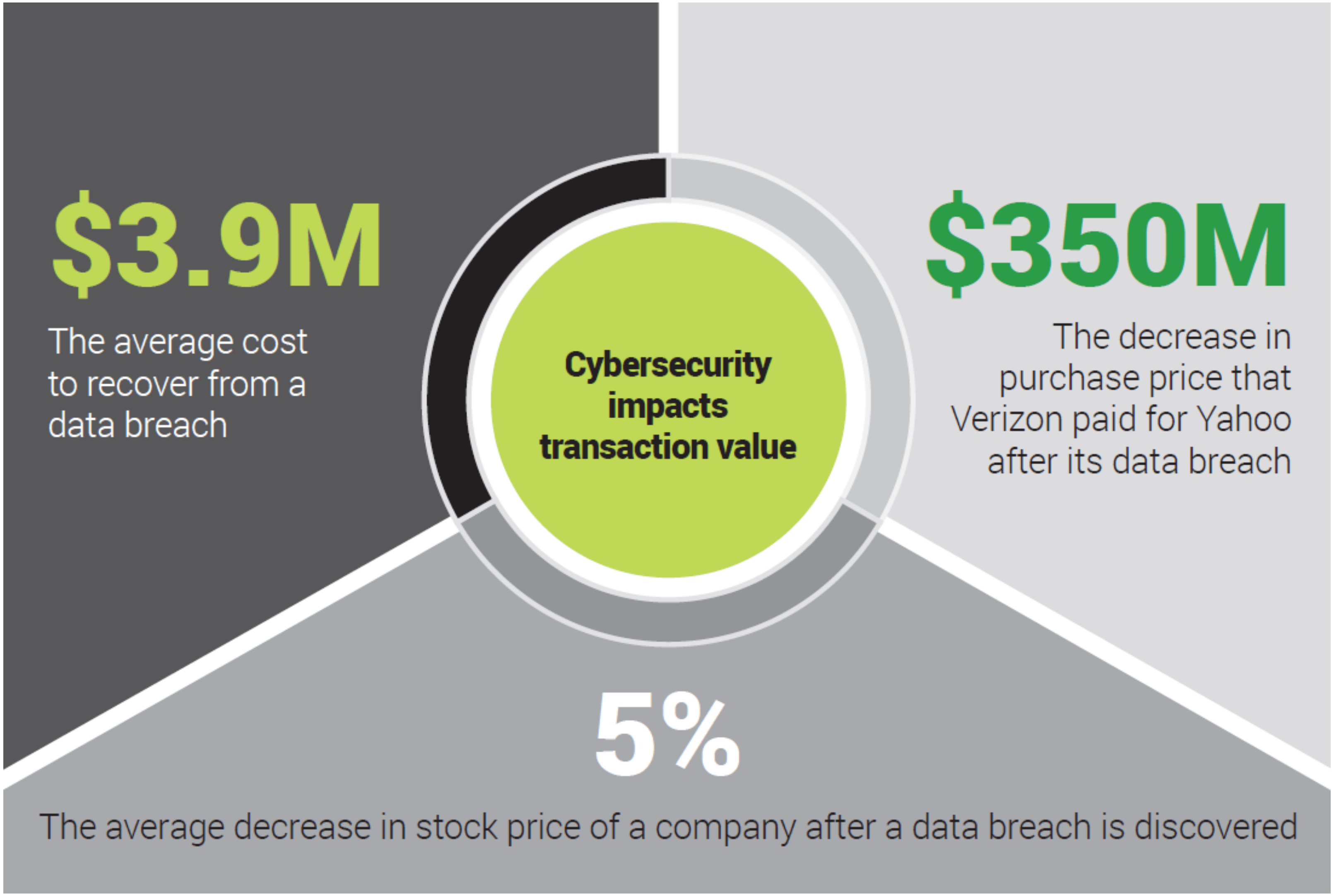
2/3
of cyber attacks
are targeted at small and medium sided businesses

191 days
average time to identify a breach

32%
chance of a C-suite executive being terminated after a breach

77%
of organizations do NOT have a formal incident recovery plan

60%
of small and medium sized businesses will no longer exist 6 months after a breach



Cybersecurity impacts transaction value

$3.9M

The average cost to recover from a data breach

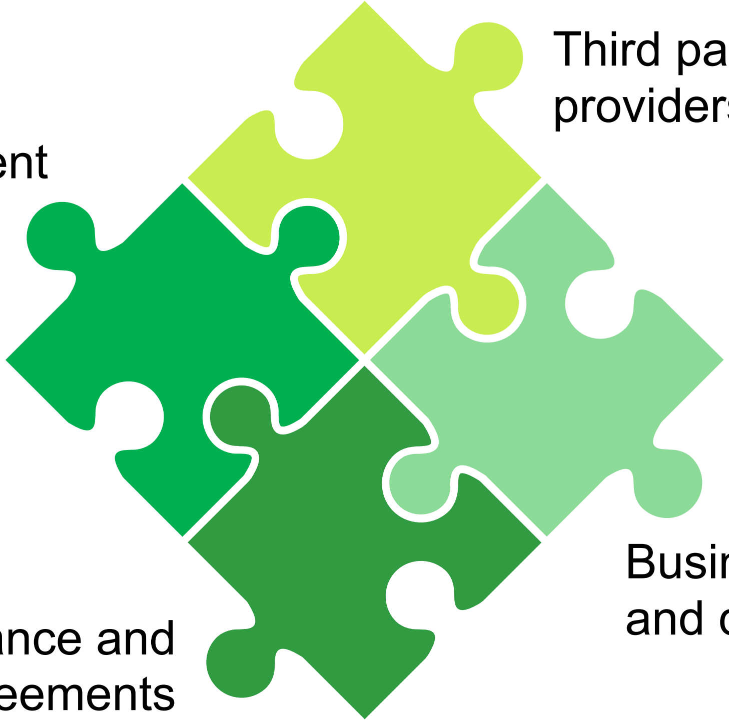
$350M

The decrease in purchase price that Verizon paid for Yahoo after its data breach

5%

The average decrease in stock price of a company after a data breach is discovered

Cyber isn't the only risk



IT asset management

Third party service providers

Business continuity and disaster recovery

Hardware maintenance and software licensing agreements

Polling question #1

Do your portfolio companies provide healthcare, retail, or manufacturing services?

a. Yes
b. No

What is a technology due diligence assessment?

Types of technology diligence assessments

“RED FLAGS” ASSESSMENT

Quick assessment to identify immediate risks

FULL SCOPE TECHNOLOGY DUE DILIGENCE

Deep review of a target’s IT and security environment and risks

Performing a technology diligence assessment

When performing a technology diligence assessment, our team follows these steps:

- Interviews with key IT personnel and service providers
- Identification of technology assets (hardware and software)
- Identification of datacenter locations and cloud hosting services
- Analysis of hardware maintenance and software licensing agreements
- Benchmarking of current organization structure & IT spend
- Review of third party service provider costs, SLAs and security controls
- Review of security solutions currently in place & previous risk assessments
- Determination of synergies or constraints during integration post-acquisition
- Review of business continuity and disaster recovery plans

Key post-acquisition considerations

INTEGRATION

STAND ALONE OPERATION

bakertilly
now, for tomorrow.

Case Studies

CASE STUDY 1

Manufacturing acquisition

Background

Assessed the IT environment and associated security controls with a manufacturing company and its subsidiaries.

Assessment

- The target was using a third party IT service provider and the service provider was effectively managing their IT environment
- However, a subsidiary of the target wasn’t using the service provider.
  - One IT staff member
  - Windows 2000 server connected to the internet
  - Windows XP workstations running the manufacturing equipment
  - Insecure storage of customer credit card numbers
  - Use of shared accounts and password

Impact

The cost of re-architecting and implementing new IT hardware/software was estimated at over $100,000, and additional ongoing costs were incurred for the IT service provider to manage the subsidiary’s environment.

CASE STUDY 2

Lighting design company

Background

Assessed the IT environment and associated data security controls, for a company that produces lighting and signage designs.

Assessment

- The purchasing company wanted to integrate the lighting design company into their operations. However, the target also provided services to various competitors of the purchasing company.
- In order to help the viability of the transaction, our team:
  - Assessed the current IT environment and data security controls; and
  - Designed a future state environment that would protect each client’s information and proprietary designs, without impacting manufacturing operations of the lighting and signage.

Impact

Based on our findings and recommendations, the acquiring company was able to see a path forward to ensure the privacy of their client’s personal information, as well as the protection of each client’s proprietary designs. Without this comfort, the transaction may not have occurred.

CASE STUDY 3

Marketing company

Background

Assessed the IT environment and associated security controls, for a company that provides hosted marketing services, including consumer mailings.

Assessment

- The marketing company hosted the domains of multiple clients in a third party web-hosting environment and maintained a privacy policy for the collection, storage and use of consumer information.
- Our team identified a general lack of documented processes or ad-hoc documentation that was put together based on our requests. While ad-hoc documentation is not abnormal in smaller organizations, the increased pressure from state legislatures on the protection of consumer information has increased the need for organizations to maintain well documented processes on the collection, storage and processing of consumer information.
- Recent legislation out of California (the California Consumer Privacy Act (CCPA)) has significantly increased the liability organizations face if consumer information is not properly protected or consumer data is misused.

Impact

Based on our findings and recommendations, the acquiring company has begun the process to perform additional data privacy assessments and thoroughly document privacy processes to ensure they are in alignment with the privacy legislation in the U.S.

Polling question #2

How prepared are you in regards to emerging data privacy regulations (e.g. CCPA)?

a. Very prepared
b. Somewhat prepared
c. Not at all prepared
d. Not sure

Managing IT and cyber risks post-acquisition

Take a risk-based approach

1 Take an inventory of your business assets (hardware, software, data, locations, people, and processes) and identify the criticality of each asset

2 Identify the risks associated with your business and the assets that support your business (e.g. risk of an insider stealing trade secrets or a hacker stealing/selling the personal information of your employees and customers)

3 Prioritize your investments to align with the risks you have identified and the criticality of the business asset

Be aware of who you do business with

Business today is not performed in a silo, most organizations have multiple business partners that they use to perform specific business functions. These third parties introduce risk to your business that you may not even be aware of.

- **Identify the third party vendors/suppliers** that you have a business relationship with, and then identify the risk that vendor potentially poses to your reputation (e.g. Do they process payroll information? Do they have access to your network? Do they send marketing material to your customers?)

- **Perform risk assessments** on your most critical third party vendor relationships and ensure that your contractual agreements have security requirements clearly identified in the agreement

- If the vendor provides you an IT service (such as outsourced payroll processing) require that vendor to get a third party assessment on an annual basis. These assessments come in the form of the **SOC 1** or **SOC 2** reports (System and Organization Controls)

Build a security aware culture

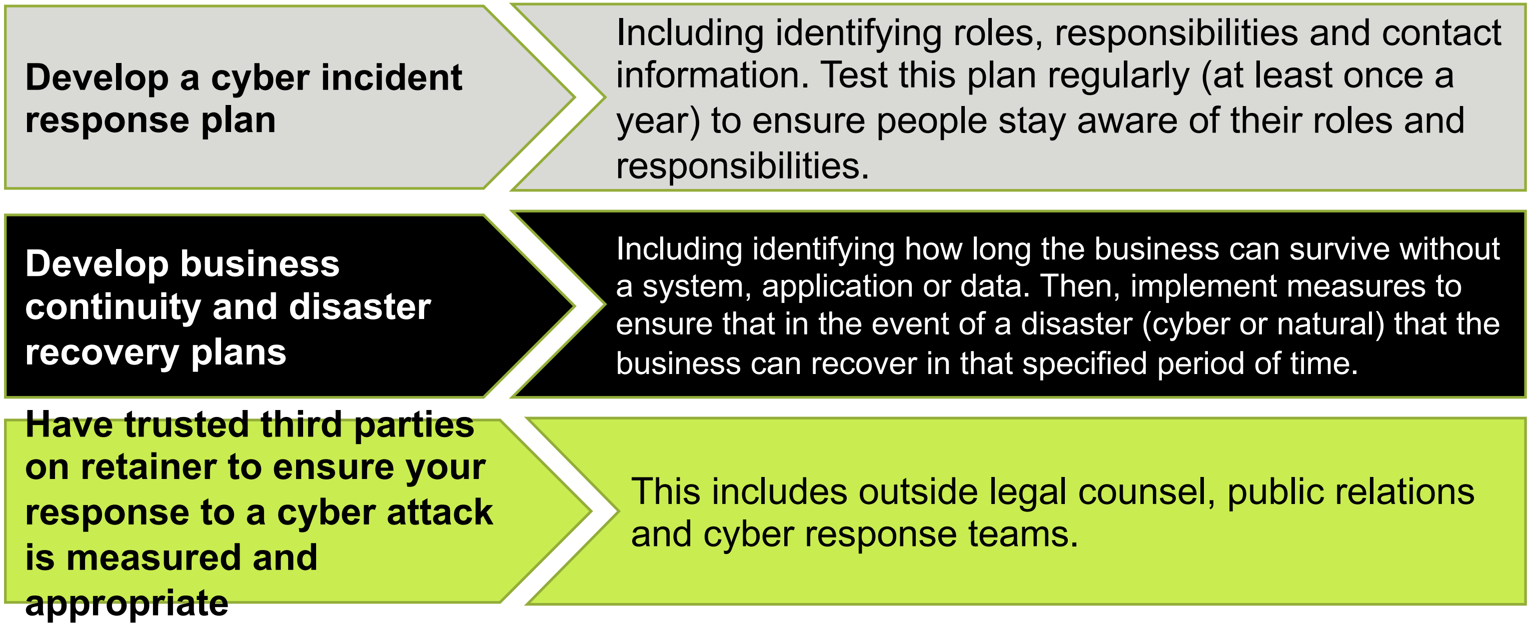
Protecting your organization is not all about the technology. People are a major contributing factor to whether you will suffer a data breach. Users are being targeted every day and many organizations are falling victim to malware or ransomware infections due to the lack of cybersecurity awareness of their end users.

- **Employee onboarding** should include discussion on security expectations (e.g. not sharing passwords, locking your computer when you step away, protecting sensitive company information). You should also provide new employees the information security policy to review and sign-off that they have actually read the policy

- Organizations support **ongoing security awareness** through internal marketing emails, posters and an annual security refresher
- Additionally, due to the increased use of phishing to compromise organizations, you should implement **phishing campaigns** to test users and increase their awareness of the threat vector

Enhance your resiliency to a cyber attack

You have to start planning for a cyber attack today. Organizations that have an incident response plan that they test regularly are better suited to weather the storm and minimize impact to reputation and loss of customer confidence.



Develop a cyber incident response plan

Including identifying roles, responsibilities and contact information. Test this plan regularly (at least once a year) to ensure people stay aware of their roles and responsibilities.

Develop business continuity and disaster recovery plans

Including identifying how long the business can survive without a system, application or data. Then, implement measures to ensure that in the event of a disaster (cyber or natural) that the business can recover in that specified period of time.

Have trusted third parties on retainer to ensure your response to a cyber attack is measured and appropriate

This includes outside legal counsel, public relations and cyber response teams.

Polling question #3

How effectively do you feel you are managing your IT and cyber risks across your portfolio companies?

a. Very effectively
b. Somewhat effectively
c. Not at all effectively
d. Not sure

Q & A

bakertilly
now, for tomorrow.

ADDITIONAL SERVICES AND RESOURCES

Connect with us

Bill Chapman
Partner
Transaction advisory services
william.chapman@bakertilly.com
312-729-8020

Atit Shah
Partner
Risk, internal audit and cybersecurity
atit.shah@bakertilly.com
972-748-0491

Brian Nichols
Director
Risk, internal audit and cybersecurity
brian.nichols@bakertilly.com
972-748-0496

bakertilly.com/cybersecurity

bakertilly
now, for tomorrow.

Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly Virchow Krause, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities.

Baker Tilly’s cybersecurity services

Advisory

- Strategic cyber advisory
- Cybersecurity policy & program development
- Cybersecurity risk assessments & cyber health checks
- Breach response preparedness planning
- Cybersecurity compliance readiness
- Pre-loss risk assessment
- Cyber risk insurance analysis
- Crisis claims consulting
- Business interruption risk advisory

Operations

- Virtual Chief Information Security Officer (CISO)/ Chief Technology Officer (CTO)
- Cybersecurity program design and implementation
- Integrated security testing services
- Cybersecurity monitoring services
- Incident response services
- Cybersecurity remediation services
- Penetration testing and vulnerability scanning
- Cyber hunting services
- SIEM content/tuning services

Education

- Security education and awareness programs
  - Board security education
  - Cyber hygiene
  - Social engineering
  - Phishing
  - Ransomware
- Simulation, exercises and war games
  - Board crisis exercises
  - Breach management
  - Tabletop exercises
  - Red team

Governance

- IT project risk reviews
- IT risk assessments
- IT effectiveness assessments
- Business continuity planning, management and testing
- Disaster recovery programs
- Supplier risk interruption (external risk)
- Compliance program assessments

Assurance

- HITRUST validation
- IT audit
  - Outsourcing
  - Co-sourcing
- IT SOX
  - Readiness
  - Testing
- System and Organization Controls (SOC) reporting
  - SOC for Cybersecurity
  - SOC 1 and 2
  - SOC 2 + HITRUST
  - SOC for Supply Chain
- Technology due diligence

Baker Tilly's cybersecurity services (cont.)

We address all of the following regulatory programs, customizing services to the client's required needs:

- Defense Federal Acquisition Regulations Supplement (**DFARS**) for Cybersecurity
- Family Education Rights and Privacy Act (**FERPA**)
- Federal Information Security Modernization Act (**FISMA**)
- General Data Protection Regulation (**GDPR**)
- Gramm-Leach Bliley Act (**GLBA**)
- Health Insurance Portability and Accountability Act (**HIPAA**)
- International Organization for Standardization (**ISO**) 27001
- Model Audit Rule
- NAIC Insurance Data Security Model Act
- National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (**CSF**)
- New York Department of Financial Services (**NY DFS**) Cybersecurity Regulation
- Payment Card Industry Data Security Standard (**PCI DSS**)

Baker Tilly's data privacy services

Assessment

Privacy compliance readiness assessments

Privacy risk assessments

Privacy certifications (HIPAA, HITRUST)

Validation (Privacy Shield)

Advisory

Strategic privacy advisory services

Virtual Data Protection Officer (VDPO)

Ad-hoc consulting

Education

Privacy education and awareness programs

Board privacy education

Execution

Privacy program design services

Privacy remediation services

Policy and process creation / review

We address all of the following regulatory programs, customizing services to the client's required needs:

- California Consumer Privacy Act (CCPA)
- Family Education Rights and Privacy Act (FERPA)
- General Data Protection Regulation (GDPR)
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- HITRUST
- Payment Card Industry Data Security Standard (PCI DSS)
- Privacy Shield
- Regulation P
- System and Organization Controls (SOC)