

Cybersecurity Technology Transfer to Practice (TTP)

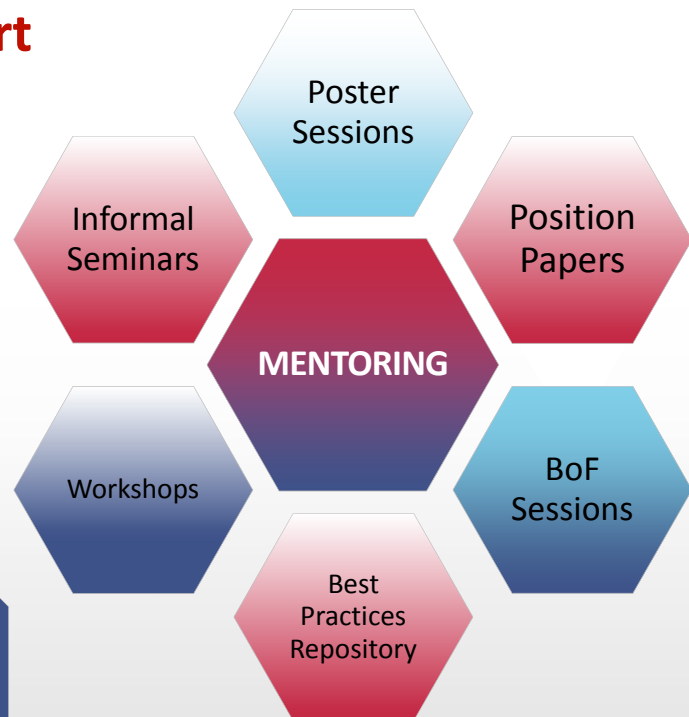
PIs: Dr. Alec Yasinsac, Ms. Rebecca Bace, Dr. Michael Chambers

<http://soc.southalabama.edu/ttp/>

A Network of TTP Support & Resources

Obstacles to TTP can include:

- Finding the right enterprise partners
- Gathering significant datasets
- Navigating institutional obstacles
- Building production quality code
- Establishing support for open source software



The Solution: A Proposal to NSF SaTC, TTP Designation.

The Core Problem

Security research that COULD transition to practice, but hasn't.

For PIs

Why engage in tech transfer?

- Increase the impact of your research
- Access industry funding and form research collaborations
- Produce commercial products (and associated profit) from research results

TTP Project Examples

- IUUC/ICSI / Bro
- Dakota St / Access Control Testing
- NYPoly / Secure Python
- UC Berkeley / User Centric Mobile Privacy
- Boston U / A Modular Approach to Cloud Security
- UCSD / Detection & Analysis of Large Scale Internet Outages
- UAB / Secure & Trustworthy Provenance for Accountable Clouds



NSF SaTC

Sign up for mentoring and/or to be a mentor at <http://tinyurl.com/j9j6aee>

NSF SaTC Submission deadlines: MED: 10/19 annually; SM 11/16 annually

Visit NSF SaTC and the TTP Ecosystem websites to learn more.

Contact us at ttp@southalabama.edu.



TTP Ecosystem



National Science Foundation
WHERE DISCOVERIES BEGIN



UNIVERSITY OF
SOUTH ALABAMA

Presenter Bios

Rebecca Gurley Bace



Becky Bace is Chief Strategist for the Center for Forensics, Information Technology and Security (CFITS) at the University of South Alabama, and President/CEO of Infi-del, Inc., a strategic consulting practice specializing in cyber security. She has, over her thirty-year career in IT Security, served in numerous operational, technical and business executive roles, including Research Program Director for NSA, where she sponsored and supervised much of the seminal research in Intrusion Detection. She was Venture Consultant for Trident Capital, a tier 1 Venture Capital firm headquartered in Palo Alto, CA; while there, she served as resident cyber security technologist and worked with the firm to build and industry-leading portfolio of security startups. Bace also served as Technical VP of the Cyber Security Practice for In-Q-Tel, the investment arm of the U.S. Intelligence Community. At IQT, she built, and then managed a team of security thought leaders and investment professionals who leveraged commercial security product capabilities in order to meet mission needs in the area.

Bace has been named as one of the most influential women in IT security over the last decade.

Her writing credits include two textbooks, chapters contributed to five others (including the last three editions of the practice handbook for the Information Security profession) and a NIST special publication on Intrusion Detection and Response.



Michael Chambers

In November 2015 the University of South Alabama (USA) named Dr. Michael Chambers to the newly created position of Assistant Vice President for Research Innovation. Before joining USA, Dr. Chambers founded and served as President and CEO of Swift Biotech, a company developing screens and diagnostics for gynecological cancers. The core technology received a substantial grant from the National Institutes of Health and was awarded in 2013 the Eugene Bricker Award for *Best Global Research* by the International Society of Pelvic Surgeons.

Before Swift, Chambers helped found and led InnoRx Pharmaceuticals (ocular drug delivery) as CEO until negotiating its sale to SurModics (NASDAQ: SRDX). Prior Chairman of ProUroCare, a public company based in Minneapolis, he has also served on the boards of InQ Biosystems, Gene Capture, BioAlabama and the [Eco-nomic Development Partnership of Alabama](#). He founded the Gulf Coast Angel Network, co-founded 1702 (an entrepreneurship and mentoring organization) and was named "Start-Up Executive of the Year" in 2014 by Alabama LaunchPad.

He received B.A. and J.D. degrees from the University of Alabama and a Ph.D. from the University of Geneva in Switzerland where he was a Rotary Ambassadorial Scholar and a Swiss Confederation Fellow. He has previously been recognized in the *Best Attorneys in the United States* in Commercial Law and a *Top Attorney in Health Care*. Dr. Chambers has also been selected as a grant reviewer by the National Science Foundation.



TTP

CYBER

INDUSTRY

ACADEMIA

GOVERNMENT

THE CORE PROBLEM:

Security research that
COULD be part of
tech transfer, but isn't.



NSF SaTC Website

To learn more contact
ttp@southalabama.edu



TTP Ecosystem Website

NSF Secure and Trustworthy Cyberspace (SaTC)

Secure and Trustworthy Cyberspace is one of the perennial programs in NSF's CISE directorate (Computer and Information Science and Engineering). See solicitation at: https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709

Eligibility for TTP Program

Transitioning successful research into practice is one of six critical areas to successful cybersecurity R&D as identified by the Federal Cybersecurity Research and Development Strategic Plan. Proposals must be submitted pursuant to one of four designations, one of which is Transition to Practice. The TTP designation is for "proposals that are focused exclusively on transitioning *existing research results* to practice." The TTP designation may only be used for Small and Medium proposals (not Large or EDU). Two and four year institutions with a US campus and non-academic entities are eligible. Software developed need not be open source, but a strong case must be provided justifying this approach. If open source, it should be released under the open source license listed by the Open Source Initiative (<http://www.opensource.org/>). Software developers are encouraged to ~~utilize~~ utilize vulnerability analysis scanning tools throughout the development process and describe the software assurance best practices that will be followed. A TTP proposal must include a project plan that addresses system development milestones and an evaluation plan for the working system.

Deadlines

October 19 (annually) for Medium proposals: \$500,001—\$1,200,000, up to 4 years
November 16 (annually) for Small proposals: up to \$500,000, up to 3 years

Purpose of TTP Grants

"The objective of the Transition to Practice (TTP) designation is to **support the development, implementation, and deployment of later-stage and applied security research into an operational environment**. A TTP-designated proposal must specifically describe how the successful research results will be further developed and deployed in organizations or industries, including in networks and end systems. Collaborations with industry are strongly encouraged. The outcome of a TTP project is not intended to be solely commercialization. A TTP may be a stepping-stone to a Small Business Innovation Research (SBIR) activity by means of a proof of concept. A TTP may transition later-stage research by a number of other means."

To Learn More About TTP Opportunities with SaTC

FAQs: <http://www.nsf.gov/pubs/2015/nsf15010/nsf15010.jsp>

TTP Ecosystem website for more information: <http://soc.southalabama.edu/ttp/>

Sign up for services and/or to be a TTP mentor: <http://tinyurl.com/j9j6aee>

For More Information Contact: Dr. Alec Yasinsac

Dean and Professor

University of South Alabama School of Computing

ttp@southalabama.edu | 251-460-6390



Secure and Trustworthy Cyberspace (SaTC)

PROGRAM SOLICITATION

NSF 16-580

REPLACES DOCUMENT(S):

NSF 15-575



National Science Foundation

Directorate for Computer & Information Science & Engineering
Division of Computer and Network Systems
Division of Computing and Communication Foundations
Division of Information & Intelligent Systems
Division of Advanced Cyberinfrastructure

Directorate for Social, Behavioral & Economic Sciences
Division of Social and Economic Sciences
Division of Behavioral and Cognitive Sciences

Directorate for Mathematical & Physical Sciences
Division of Mathematical Sciences

Directorate for Engineering
Division of Electrical, Communications and Cyber Systems

Directorate for Education & Human Resources
Division of Graduate Education



Semiconductor Research Corporation

Submission Window Date(s) (due by 5 p.m. submitter's local time):

October 12, 2016 - October 19, 2016

October 12 - October 19, Annually Thereafter

LARGE Projects

October 12, 2016 - October 19, 2016

October 12 - October 19, Annually Thereafter

MEDIUM Projects

November 02, 2016 - November 16, 2016

November 2 - November 16, Annually Thereafter

SMALL Projects

December 01, 2016 - December 15, 2016

December 1 - December 15, Annually Thereafter

CYBERSECURITY EDUCATION Projects

IMPORTANT INFORMATION AND REVISION NOTES

Revision Summary: This is a revision of [NSF 15-575](#), the solicitation for the SaTC Program. The revisions include:

1. Revisions to the submission deadline windows;
2. Revisions to the SaTC program description, including (a) replacement of perspectives with designations; (b) addition of topic areas; and (c) change to STARSS procedure to include parallel submission to and review by SRC;
3. Revisions to the Proposal Preparation Instructions;
4. Changes to eligibility information regarding (a) who may submit a proposal and (b) number of proposals per PI or Co-PI; and
5. Under Additional Solicitation Specific Review Criteria, reviewers are now asked to provide specific evaluation of whether key personnel, and especially lead PIs, have allocated adequate time for both their individual technical contributions and the leadership of collaborative activities necessary to realize the synergistic effects of larger-scale research.

The following recent revisions to the *Grant Proposal Guide (GPG)* will be closely observed for all submissions to this solicitation:

- GPG Chapter II.C.2.d.i requires that, "The Project Description must contain, as a separate section within the narrative, a section labeled 'Broader Impacts'."

- GPG Chapter II.C.2.f clarifies the requirements for Biographical Sketch(es).
- GPG Chapter II.C.2.h revises requirements for reporting Current and Pending Support.
- GPG Chapter II.C.2.j, Special Information and Supplementary Documentation, specifies the proper scope for letters of collaboration.

Any proposal submitted in response to this solicitation should be submitted in accordance with the revised *NSF Proposal & Award Policies & Procedures Guide (PAPPG) (NSF 16-1)*, which is effective for proposals submitted, or due, on or after January 25, 2016.

SUMMARY OF PROGRAM REQUIREMENTS

General Information

Program Title:

Secure and Trustworthy Cyberspace (SaTC)

Synopsis of Program:

In today's increasingly networked, distributed, and asynchronous world, cybersecurity involves hardware, software, networks, data, people, and integration with the physical world. Society's overwhelming reliance on this complex cyberspace has, however, exposed its fragility and vulnerabilities: corporations, agencies, national infrastructure and individuals have been victims of cyber-attacks. Achieving a truly secure cyberspace requires addressing both challenging scientific and engineering problems involving many components of a system, and vulnerabilities that arise from human behaviors and choices. Examining the fundamentals of security and privacy as a multidisciplinary subject can lead to fundamentally new ways to design, build and operate cyber systems, protect existing infrastructure, and motivate and educate individuals about cybersecurity.

The goals of the Secure and Trustworthy Cyberspace (SaTC) program are aligned with the [Federal Cybersecurity Research and Development Strategic Plan \(RDSP\)](#) and the [National Privacy Research Strategy \(NPRS\)](#) to protect and preserve the growing social and economic benefits of cyber systems while ensuring security and privacy. The RDSP identified six areas critical to successful cybersecurity R&D: (1) scientific foundations; (2) risk management; (3) human aspects; (4) transitioning successful research into practice; (5) workforce development; and (6) enhancing the research infrastructure. The NPRS, which complements the RDSP, identifies a framework for privacy research, anchored in characterizing privacy expectations, understanding privacy violations, engineering privacy-protecting systems, and recovering from privacy violations. In alignment with the objectives in both strategic plans, the SaTC program takes an interdisciplinary, comprehensive and holistic approach to cybersecurity research, development, and education, and encourages the transition of promising research ideas into practice.

The SaTC program welcomes proposals that address cybersecurity and privacy, and draw on expertise in one or more of these areas: computing, communication and information sciences; engineering; economics; education; mathematics; statistics; and social and behavioral sciences. **Proposals that advance the field of cybersecurity and privacy within a single discipline or interdisciplinary efforts that span multiple disciplines are both encouraged.**

Proposals may be submitted in one of the following three project size classes:

- Small projects: up to \$500,000 in total budget, with durations of up to three years;
- Medium projects: \$500,001 to \$1,200,000 in total budget, with durations of up to four years;
- Large projects: \$1,200,001 to \$3,000,000 in total budget, with durations of up to five years.

In addition to the project size classes, proposals must be submitted pursuant to one of the following designations, each of which may have additional restrictions and administrative obligations as specified in this program solicitation.

- CORE: The main focus of the SaTC research program, spanning the interests of NSF's Directorates for Computer and Information Science and Engineering (CISE), Engineering (ENG), Mathematical and Physical Sciences (MPS), and Social, Behavioral and Economic Sciences (SBE). Interdisciplinary proposals are welcomed to CORE.
- EDU: The Education (EDU) designation will be used to label proposals focusing entirely on cybersecurity education. *Note that proposals that are designated as EDU have budgets limited to \$300,000 and durations of up to two years.*
- STARSS: The Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) designation will be used to label proposals that are submitted to the joint program focused on hardware security with the Semiconductor Research Corporation (SRC). *The STARSS designation may only be used for Small proposals. This designation has additional administrative obligations.*
- TTP: The Transition to Practice (TTP) designation will be used to label proposals that are focused exclusively on transitioning existing research results to practice. *The TTP designation may only be used for Small and Medium proposals.*

Cognizant Program Officer(s):

Please note that the following information is current at the time of publishing. See program website for any updates to the points of contact.

- Nina Amla, Program Director, CISE/CCF, 1110, telephone: (703) 292-8910, email: namla@nsf.gov
- Sol Greenspan, Program Director, CISE/CCF, 1115, telephone: (703) 292-8910, email: sgreensp@nsf.gov
- Timothy Hodges, Program Director, MPS/DMS, 1020, telephone: (703) 292-2113, email: thodges@nsf.gov
- Dongwon Lee, Program Director, EHR/DGE, 865, telephone: (703) 292-4679, email: dlee@nsf.gov

- Wenjing Lou, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: wlou@nsf.gov
- Anita Nikolich, Program Director, CISE/ACI, 1145, telephone: (703) 292-8970, email: anikolic@nsf.gov
- Victor P. Piotrowski, Program Director, EHR/DGE, 865, telephone: (703) 292-5141, email: vpotrow@nsf.gov
- Andrew D. Pollington, Program Director, MPS/DMS, 1025, telephone: (703) 292-4878, email: adpollin@nsf.gov
- Deborah Shands, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: dshands@nsf.gov
- Yan Solihin, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: ysolihin@nsf.gov
- Ralph Wachter, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: rwachter@nsf.gov
- Chengshan Xiao, Program Director, ENG/EECS, ENG/ECCS, 525, telephone: (703) 292-8339, email: cxiao@nsf.gov
- Heng Xu, Program Director, SBE/SES, 995, telephone: (703) 292-8643, email: hxu@nsf.gov
- Nan Zhang, Program Director, CISE/IIS, 1125, telephone: (703) 292-8930, email: nanzhang@nsf.gov
- Celia Merzbacher, Semiconductor Research Corporation, telephone: (919) 941-9413, email: celia.merzbacher@src.org

Applicable Catalog of Federal Domestic Assistance (CFDA) Number(s):

- 47.041 --- Engineering
- 47.049 --- Mathematical and Physical Sciences
- 47.070 --- Computer and Information Science and Engineering
- 47.075 --- Social Behavioral and Economic Sciences
- 47.076 --- Education and Human Resources

Award Information

Anticipated Type of Award: Standard Grant or Continuing Grant

Estimated Number of Awards: 88

In FY 2017, NSF anticipates approximately 10 Education awards, 50 Small awards, 25 Medium awards and 3 Large awards.

Anticipated Funding Amount: \$68,300,000

per year, dependent on the availability of funds.

Eligibility Information

Who May Submit Proposals:

Proposals may only be submitted by the following:

- Universities and Colleges - Universities and two- and four-year colleges (including community colleges) accredited in, and having a campus located in, the US acting on behalf of their faculty members. Such organizations also are referred to as academic institutions.
- Non-profit, non-academic organizations: Independent museums, observatories, research labs, professional societies and similar organizations in the U.S. associated with educational or research activities.

Who May Serve as PI:

There are no restrictions or limits.

Limit on Number of Proposals per Organization:

There are no restrictions or limits.

Limit on Number of Proposals per PI or Co-PI: 5

An individual can participate as a PI, co-PI or senior personnel on no more than five SaTC proposals. There is a limit of:

- two proposals designated as CORE and/or STARSS (across Small, Medium, and Large); and
- two proposals designated as TTP (either Small or Medium); and
- one proposal designated as EDU.

These limits apply per year to Small, Medium, Large and Education proposals in response to this particular solicitation, and are unrelated to any limits imposed in other NSF solicitations. Note, for example, that you may NOT submit two proposals to SaTC CORE, and three to STARSS, but you may submit one proposal to SaTC CORE, another to STARSS, two to TTP and one to EDU.

These eligibility constraints will be strictly enforced in order to treat everyone fairly and consistently. In the event that an individual exceeds this limit, proposals received within the limit will be accepted based on earliest date and time of proposal submission. **No exceptions will be made.**

Proposal Preparation and Submission Instructions

A. Proposal Preparation Instructions

STARSS provides an opportunity for close collaboration with industry through SRC. Hardware security proposals not specifically addressing STARSS criteria (see Section VI) should be submitted to the SaTC CORE designation. When considering topics for research, proposers are encouraged to review past awards made by the STARSS activity and identify areas that are within the technical scope and not already the subject of study. Proposals in areas not already covered by prior projects are particularly encouraged. To find past STARSS awards, go to <http://www.nsf.gov/awardsearch> and search for "STARSS."

Questions regarding SRC policies and guidelines should be addressed directly to Celia Merzbacher, Semiconductor Research Corporation, at (919) 941-9413 or celia.merzbacher@src.org.

Transition to Practice (TTP) Designation

The objective of the Transition to Practice (TTP) designation is to support the development, implementation, and deployment of later-stage and applied security research into an operational environment. A TTP-designated proposal must specifically describe how the successful research results will be further developed and deployed in organizations or industries, including in networks and end systems. Collaborations with industry are strongly encouraged. The outcome of a TTP project is not intended to be solely commercialization. A TTP may be a stepping-stone to an Small Business Innovation Research (SBIR) activity by means of a proof of concept. A TTP may transition later-stage research by a number of other means.

A TTP proposal must include a project plan that addresses system development milestones and an evaluation plan for the working system.

In addition, TTP proposals will be evaluated with careful attention to the:

- Description of the problem being solved or need being addressed;
- Identification of a target user group or organization that will serve as an early adopter of the technology; if no early adopter is identified by the time the proposal is submitted, the proposal must specify milestones as to when an early adopter will be named;
- Deployment plan for implementing the capability or prototype system into an operational environment;
- Novelty of the intended system, software, or architecture;
- Composition of the proposal team, which should demonstrate not only technical expertise in areas such as software engineering, but also skills in project management and systems development;
- Explanation of the post-grant, long-term software and/or system sustainability;
- Appropriateness of the budget for the effort; and
- Extent of collaboration with the university Technology Transfer Office (TTO) or similar organization from the PI's institution (a letter from the TTO or similar organization indicating its willingness to support the proposal is strongly encouraged).

Software developed under the TTP designation is not required to be open source. However, if open source software is developed, it should be released under the open source license listed by the Open Source Initiative (<http://www.opensource.org/>). If software will not be open source, a strong case must be provided justifying this approach. Software developers are encouraged to demonstrate utilization of vulnerability analysis scanning tools throughout the development process and describe the software assurance best practices that will be followed.

Questions regarding the Transition to Practice (TTP) designation should be addressed directly to SaTC Program Officer Anita Nikolich in the Division of Advanced Cyberinfrastructure (ACI) at anikolic@nsf.gov.

Cybersecurity Education (EDU) Designation

On occasion, the results of SaTC-funded research lead to widespread changes in our understanding of the fundamentals of cybersecurity that can, in turn, lead to fundamentally new ways to motivate and educate students about cybersecurity. Proposals submitted to this designation leverage successful results from previous and current basic research in cybersecurity and research on student learning, both in terms of intellectual merit and broader impacts, to address the challenge of expanding existing educational opportunities and resources in cybersecurity. This might include but is not limited to the following efforts:

- Based on the results of previous and current basic research in cybersecurity, define a cybersecurity body of knowledge and establish curricular recommendations for new courses (both traditional and online), degree programs, and educational pathways leading to wide adoption nationally;
- Evaluate the effects of these curricula on student learning;
- Encourage the participation of a broad and diverse population in Cybersecurity Education;
- Develop virtual laboratories to promote collaboration and resource sharing in Cybersecurity Education;
- Develop partnerships between centers of research in cybersecurity and institutions of higher education that lead to improved models for the integration of research experiences into cybersecurity degree programs;
- Develop and evaluate the effectiveness of cybersecurity competitions, games, and other outreach and retention activities; and
- Conduct research that advances improvements in teaching and student learning in cybersecurity and, where possible, focuses on broadening participation.

Cybersecurity Education proposal budgets are limited to \$300,000 and their durations are limited to two years.

Questions about Cybersecurity Education proposals should be addressed directly to SaTC Program Officer Victor Piotrowski in the Directorate for Education and Human Resources (EHR) at vpiotrow@nsf.gov.

SaTC PI MEETINGS

The SaTC program plans to host PI meetings every other year with participation from all active SaTC projects. This meeting will be a community-wide event with representatives from federal agencies, academia, industry, and international institutions. Principal investigators from all solicitation designations are expected to participate in these meetings.

For Small, Medium and Education awards, one or more project representatives (PI/co-PI/senior researcher, or NSF-approved replacement) must attend the first PI meeting held after the beginning of the award. For Large awards, one or more project representatives (PI/co-PI/senior researcher, or NSF-approved replacement) must attend every PI meeting held throughout the duration of the grant. These requirements apply to collaborative proposals as a whole, not to each institution within a project.

In addition, in years in which no SaTC PI meeting is held, SRC will hold a review of all Small STARSS-designated projects.

EMBEDDED REU SUPPLEMENTS

The *Research Experiences for Undergraduates (REU): Sites and Supplements* solicitation (NSF 13-542) gives instructions for embedding a request for a REU Supplement in a proposal. Proposers are invited to embed a request for a REU Supplement in the typical amount for one year only according to standard guidelines (detailed below). The amounts of the REU Supplements do not

FAQ for NSF 14-599 (most recent version)

TRANSITION TO PRACTICE (TTP)

Q. Can a STARSS perspective proposal include a Transition to Practice (TTP) Option?

A. Yes. A STARSS perspective proposal is like any other Small proposal, and may include a TTP Option.

Q. Is the TTP Perspective that was present in the FY12 solicitation still available?

A. No. Transition to Practice (TTP) options are available, but not the perspective.

Q. Is it expected that work pursuant to the TTP Option will occur only at the end of a project?

A. Not necessarily. Although Transition work often does come toward the end of a project, after preliminary work is successfully completed, other project schedules are possible. For example, a project could be iterative, whereby research and transition activities alternate, each activity building upon the previous work. Software development might be done in a similarly iterative manner. A basic project plan with general milestones is helpful when added as part of the five-page TTP Option Supplementary Document.

Q. Software developed under the TTP Option must be open source. Does that requirement apply to all software developed under any SaTC award?

A. No. The open source requirement applies only to software developed under the TTP Option, but not to the base grant. However, the open source requirement for the TTP Option may be waived on a case by case basis.

Q. What is the relationship between SaTC's TTP and NSF's I-Corps program?

A. The programs are independent and have different structures, though both aim to help bring the fruits of research projects to general use. Award sizes, scope and duration are different. Please see the solicitations for details and consult NSF Program Officers if you have questions.

<https://www.nsf.gov/pubs/2015/nsf15010/nsf15010.jsp>

Transfer to Practice Scenarios

Scenario 1:

Dr. Sam Science intends to file a small TTP proposal for \$600,000 to cover expenses in his proposed budget over a five year period. He intends to file on December 1 next year because his research results will be complete as of November 16. His proposal outlines what he expects the final results will be and intends to file a TTP proposal later that will address the use of vulnerability analysis scanning tools and software best practices.

What advice would you give him concerning the TTP grant?

Scenario 2:

Dr. Helen Hacker wants to file a TTP grant for \$400,000 by December 20 next year covering a four year budget. She is concerned that she has not demonstrated proof of concept with her technology. She is able to describe her current research results and how they could be further developed and deployed in organizations or private industries, including in networks and end systems. Her dean discourages her application because she needs funding for further development, her technology is not ready for commercialization, and is probably only of interest to the government as opposed to private industry. He encourages her instead to file a SBIR in order to further develop her technology by demonstrating proof of concept and creating an implementation plan, and then the file for a TTP grant. He also chides her for sharing some of the research with a local private company under a NDA (non-disclosure agreement) and tells her that no collaboration should be pursued until after both the SBIR and TTP grant funding is awarded.

Do you agree or disagree with the advice given by the dean and why?

Scenario 3:

Peter Profit was an undergraduate student at Hack U and selected to work on a software project as the primary coder. He was paid in part and received partial academic credit for his work. His pay and the funding to his supervising professor, Dr. Dinero, was provided through a university-private sector collaboration that received matching funds from the federal government. The project was a cyber-security software program designed to protect the personal data of patients in the university health care system.

After the semester ended the project was abandoned by everyone when it was only 95% complete. Peter then became a grad student and he and Dr. Dinero resurrected the project. Peter worked without pay on the project at home using a university provided laptop. Dr. Dinero decreased Peter's teaching and counseling hours and promised him an excellent reference if he did a good job. Under Dr. Dinero's supervision, Peter completed the original program. They modified it slightly with a novel algorithm that would facilitate selection and matching of candidates for clinical trials from multiple sites. Company A, not a member of the earlier collaboration, as well as a government agency, have expressed an interest in licensing the program, but each wants to confirm that neither the university, nor anyone else, might have an ownership interest. A question has arisen about who owns the technology and what the percentage interest of ownership is.

What advice would you give Dr. Dinero on how to answer Company A's questions?

Scenario 4:

Create a Business Thesis in your group with the Auto Pilot vehicle plug in from slide presentation. Or, if one of you is working on a particular project that you can share, create a business thesis for your technology.

Appoint one person from your group to be your spokesperson. The spokesperson can be the same for all four or different for each one.

Seven Reasons Not Having a Mentor Is Costing You Money

By Travis Steffen

Say two competing entrepreneurs go head to head. Assume they have the same advantages and resources, except access to mentorship opportunities. The one with a great mentor is more likely to become more successful sooner than the one without.

While I usually don't mess around much with hypotheticals, this concept isn't exactly rocket science. However, I'd like to propose an alternate perspective, which brings to light the opportunity cost of being the entrepreneur without a mentor.

Not having a mentor could actually be costing you money. Here are 7 reasons why:

1. **You have only your own mistakes to learn from.** Sometimes mistakes are the most powerful learning tool you can have. But who says they always have to be *your* mistakes? Learning from mistakes your mentor has already made and bounced back from can provide a shortcut on your road to the right decision. Will their situations always be identical to the ones you're facing? No, but they can allow you to make much more informed decisions.
2. **People are more likely to ignore unsolicited inquiries.** If you're a relative newcomer who is very good at what you do, it may still take you years to break into your industry and partner with some of the more established heavy hitters. A cold call or email will often get tossed onto the pile. However, with an introduction provided by somebody whose name already holds water, you can get your foot in the door faster.
3. **"You are the sum of the people you associate with most."** We've all heard this before – but while we toss it around to others, few of us truly embrace it ourselves. Having someone you strive to emulate as a mentor and working hard to spend time around them and people like them can bring you closer to becoming who you really want to be.

4. **Your competitors will be quicker.** Your competitors – whether they have mentors behind them or they’re simply more established – will be able to make things happen faster than you if you are starting up without advisors by your side.

5. **You’ll waste time and money on tools and resources.** There are tons of books, courses, resources and tools out there to teach you pretty much anything. And when you’re getting started, there’s not much to guide you aside from Amazon reviews, which can be misleading. Someone with a more educated perspective can point you in the right direction right away without you having to waste valuable time and money figuring out whom and what to listen to.

6. **Opportunities will be smaller and slower.** Key partnerships and introductions will be more difficult to secure, as will gaining the trust of key brands and influencers you may want to work with to accelerate growth. A mentor can put their own reputation on the line for you should they decide you’re worthy of it. Without a mentor you will have to create your own opportunities. This will prove to be a much longer, slower road.

7. **You’ll often quit too early.** One of the most valuable things I gained from one of my mentors early on was insight about whether I should keep doing what I was doing or change my strategies entirely. Even if you’re stagnating in a certain area, growth and progress will often fail to become linear. Without a seasoned veteran telling you to stick with something despite recent events, you may give up on a project that would otherwise do exactly what you wanted it to in the long run.

Forbes on Entrepreneurs: *Seven Reasons Not Having A Mentor Is Costing You Money*; August 13, 2014; by Travis Steffen

<http://www.forbes.com/sites/theyec/2014/08/13/seven-reasons-not-having-a-mentor-is-costing-you-money/#60d253926888>



THE SEDONA CONFERENCE JOURNAL®

V o l u m e 1 7 ❖ 2 0 1 6 ❖ N u m b e r T w o

A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses

John Thomas A. Malatesta III & Sarah S. Glover

Reprinted with Permission from The Sedona
Conference Journal Volume 17, 2016, Number Two
Copyright 2016, The Sedona Conference. All Right Reserved.



ANTITRUST LAW, COMPLEX LITIGATION,
AND INTELLECTUAL PROPERTY RIGHTS

A CLEAR AND PRESENT DANGER: MITIGATING THE DATA SECURITY RISK VENDORS POSE TO BUSINESSES

*John Thomas A. Malatesta III & Sarah S. Glover**
Maynard Cooper & Gale
Birmingham, AL

“It is abundantly clear that, in many respects, a firm’s level of cybersecurity is only as good as the cybersecurity of its vendors.”

-Benjamin Lawsky, New York State Department of Financial Services Superintendent, Oct. 21, 2014.¹

Target. Home Depot. T-Mobile. What do these high-profile data breaches have in common? They were all vendor² breaches. That is, a third-party service provider served as the vehicle to these organizations’ customer data. Vendors are consistently cited as a primary cause of data breaches, and third-

* John Thomas (“J.T.”) Malatesta is the Chair of Maynard Cooper & Gale’s Cybersecurity & Privacy Practice. Sarah Glover is an associate in the group. Their practice at Maynard Cooper focuses on advising companies in the areas of cybersecurity risk management, data breach response, and privacy compliance. J.T. is a NetDiligence® Breach Coach; he guides clients through the immediate and necessary steps following a data breach, including incident response, data breach notification, regulatory inquiries and, if necessary, civil litigation.

1. Letter from Benjamin Lawsky, Former Superintendent of the N.Y. State Dep’t of Fin. Servs., to N.Y. Banks on Cybersecurity (October 21, 2014).

2. As used herein, the term “vendor” shall broadly mean any third party with which an organization has an existing or potential business relationship, recognizing that the typical vendor relationship involves the outsourcing of some function or service to another organization.

party involvement remains the highest *per capita* contributor to the cost of a data breach.³

Just ask Target. Target reported that the hackers who ultimately stole 110 million customer records in 2013 initially broke into Target's system by using credentials lifted from an HVAC vendor.⁴ From this initial access point, the hackers were eventually able to upload their malicious software to Target's point-of-sale systems, and the rest, as they say, is history. Target has reported the cost of dealing with the data breach to total \$200 million to date, reflecting \$290 million of gross expense partially offset by an insurance receivable of \$90 million.⁵

The litany of household-name breaches, along with the evolving regulatory framework governing third-party relationships, emphasize the importance of including vendor management within your enterprise risk management program, and devoting sufficient resources toward combating the cyber risk vendors present to your organization. Simply stated, vendor relationships can no longer be left in the capable hands of Information Technology to manage alone. It has evolved into an enterprise risk, prompting legal, compliance, operational risk,

3. See PONEMON INSTITUTE, 2016 COST OF DATA BREACH STUDY: UNITED STATES, at 9 (2016); PONEMON INSTITUTE, 2015 COST OF DATA BREACH STUDY: UNITED STATES 10 (2015). Thirty-six percent of businesses surveyed by the Ponemon Institute in 2014 reported data breaches caused by third party errors, glitches, or misuse. PONEMON INSTITUTE, 2014 COST OF DATA BREACH STUDY: UNITED STATES 9 (2014).

4. Brian Krebs, *The Target Breach, By the Numbers*, KREBSONSECURITY (May 6, 2014, 12:24 EST), <http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/>; Brian Krebs, *Target Hackers Broke in Via HVAC Company*, KREBSONSECURITY (Feb. 5, 2014, 13:52 EST), <http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>.

5. Target Corp., Quarterly Report (Form 10-Q), at 11 (November 25, 2015).

executive management, and other business segments to augment the risk management efforts aimed at third-party service providers.⁶

The risk vendors present to the security of an organization's sensitive data is two-fold: 1) the vendor itself could maintain the data (e.g., the medical transcription service that maintains a covered entity's patient records); or 2) the vendor does not maintain sensitive data, but could provide an access point to that data (e.g., the unidentified vendor whose stolen login credentials were used to gain perimeter access to Home Depot's systems),⁷ creating potential exposure of an entity's customer and employee personal information, financial and proprietary business information, and intellectual property. Benjamin Lawsky, the first superintendent of New York's Department of Financial Services, observed that "third-party firms can provide a backdoor entrance to hackers who are seeking to steal sensitive . . . customer data."⁸ This operational reality counsels in favor of extending vendor risk management to an organization's entire roster of vendors, contrary to the traditional model of only focusing on those vendors who specifically handle cus-

6. See, e.g., National Association of Insurance Commissioners, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (2015), http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf ("Cybersecurity transcends the information technology department and must include all facets of an organization.").

7. The Home Depot, *The Home Depot Reports Findings in Data Breach Investigation* (Nov. 6, 2014), <http://ir.homedepot.com/news-releases/2014/11-06-2014-014517315>.

8. N.Y. State Dept. of Fin. Servs., *NYDFS Report Shows Need to Tighten Cyber Security at Banks' Third-Party Vendors* (April 9, 2015), <http://www.dfs.ny.gov/about/press/pr1504091.htm>.

tomers data. The New York State Department of Financial Services (NYDFS), for example, found that the majority of banks it surveyed performed security risk assessments of their high risk vendors, such as payment processors, but did not conduct the same level of oversight for those vendors categorized as low-risk, such as office suppliers and printing companies, or for professional service providers, such as legal counsel or independent consultants.⁹

Increased regulatory scrutiny in this area further compels a more comprehensive approach to vendor management. The Payment Card Industry Security Standards Council published new guidance on third-party service provider security in August of 2014. The Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) conducted a cybersecurity preparedness examination of more than 100 registered broker-dealers and investment advisors in 2014 that focused in part on third-party risk.¹⁰ This was followed by the OCIE's 2015 Cybersecurity Examination Initiative, which again places vendor management on the short list of topics to receive heightened scrutiny.¹¹ Most recently, on September 13, 2016, the NYDFS proposed new cybersecurity regulations that would obligate financial institutions to, among other things, implement and maintain a written cybersecurity policy that addresses a number of areas, including vendor and

9. N.Y. State Dept. of Fin. Servs., *Update on Cyber Security in the Banking Sector: Third Party Service Providers*, at 3 (2015), available at http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

10. UNITED STATES SECURITIES AND EXCHANGE COMMISSION OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, *CYBERSECURITY EXAMINATION SWEEP SUMMARY*, at 1 (2015), available at <https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf>.

11. PCI SECURITY STANDARDS COUNCIL, *THIRD-PARTY SECURITY ASSURANCE* (2014), available at https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf.

third-party service provider management.¹² In an area of law that is rapidly evolving, and as businesses continue to increase the number and complexity of third-party relationships, organizations large and small would be well advised to get out in front of this issue.

The threat vendors pose to businesses is tangible. Fortunately, so are the steps a business can take to mitigate that threat. The key to vendor management—indeed any cybersecurity preparedness program—is deterrence; there is no guarantee that “doing everything right” will absolutely prevent a data breach, but implementing a comprehensive vendor management program is a formidable way to reduce the cyber risk vendor relationships introduce. This paper will examine how the law charges businesses with overseeing their vendors and how businesses are actually managing (or failing to manage) their vendors today, and it will provide practical guidance on how a business can reduce the cyber risk that vendors present.

CALL OF DUTY—WHAT IS REQUIRED OF BUSINESSES?

The exact vendor management practices that an organization must currently follow depend on the regulatory framework for that organization. Even in heavily regulated industries like financial services and healthcare, however, the law with respect to vendor management is not extensive—at least not yet. Most regulations come down in the form of general charges. The Federal Financial Institutions Examination Council’s (FFIEC) regulations implementing the Gramm-Leach-Bliley Act (GLBA) with respect to banks and other FFIEC-regulated financial institutions exemplify the three basic requirements and/or best practices that businesses should follow:

12. N.Y. State Dep’t of Fin. Servs, Proposed 23 NYCRR 500, § 500.03, available at <http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf>.

1. Exercise appropriate due diligence in selecting your service providers;
2. Require your service providers by contract to implement appropriate measures designed to meet the objectives of controlling regulatory guidelines and industry best practices; and
3. Where indicated by your risk assessment, monitor your service providers to confirm that they have satisfied their obligations¹³

These three pillars of vendor management—due diligence, contractual negotiation, and monitoring—are fleshed out below in the “battle plan” for businesses.

The legal obligations in other industries mirror the FFIEC guidelines. For example, the Health Insurance Portability and Accountability Act (HIPAA) provides that “a covered entity may permit a business associate [i.e., vendor] to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information.”¹⁴ The U.S. Department of Health and Human Services has promulgated guidance on how to comply with this general charge, providing sample contractual language to be inserted in a covered entity’s contracts with its vendors who handle protected health information.¹⁵

13. Appendix B, Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. § 570, § III(D) (2000).

14. Administrative safeguards, 45 C.F.R. § 164.308(a)(8)(b)(1).

15. U.S. Dep’t of Health & Human Servs., *Sample Business Associate Agreement Provisions* (2013), <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>.

Similarly, the National Association of Insurance Commissioners (NAIC) Standards for Safeguarding Customer Information Model Regulation, adopted by 33 states and the District of Columbia, succinctly captures these general requirements, providing that all licensees shall “[e]xercise[] appropriate due diligence in selecting [their] service providers”; and “[r]equire[] [their] service providers to implement appropriate measures designed to meet the objectives of this regulation, and where indicated by the licensee’s risk assessment, take[] appropriate steps to confirm that [their] service providers have satisfied these obligations.”¹⁶ This sentiment is echoed in the NAIC’s Principles for Effective Cybersecurity: Insurance Regulatory Guidance. (Principle 8: “[T]ake appropriate steps to ensure that third parties and service providers have controls in place to protect personally identifiable information.”)¹⁷ The new proposed NAIC model regulation actually goes one step further, requiring not only that “licensee[s] shall contract only with third-party service providers that are capable of maintaining appropriate safeguards for personal information in the licensee’s possession, custody or control,” but also that “the licensee **shall be responsible** for any failure by such third-party service providers to protect personal information.”¹⁸

16. National Association of Insurance Commissioners, Standards for Safeguarding Customer Information Model Regulation, § 8 (2002), *available at* <http://www.naic.org/store/free/MDL-673.pdf>.

17. National Association of Insurance Commissioners, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (2015), http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

18. National Association of Insurance Commissioners, Insurance Data Security Model Law, § 4(F) (2016), *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_exposure_mod_draft_clean.pdf (emphasis added).

Non-banking and non-insurance financial institutions likely fall under the catch-all jurisdiction of the Federal Trade Commission (FTC). These financial institutions are subject to the FTC Safeguards Rule implementing the GLBA, which requires businesses to “select service providers that can maintain appropriate safeguards,” “make sure [the] contract requires them to maintain safeguards,” and “oversee their handling of customer information.”¹⁹ Non-financial institutions in less regulated spheres like retail are not subject to specific cybersecurity regulations, but any business engaged in interstate commerce would still be subject to the FTC’s jurisdiction under Section 5 of the FTC Act, which the agency has used to prosecute what it deems to be insufficient data security practices, including lack of proper oversight of vendors.²⁰ Such businesses would, therefore, be well-advised to comply with the FTC Safeguards Rule and corresponding guidance.

The National Institute of Standards and Technology’s Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework), promulgated pursuant to an Executive Order of the White House in February 2014, also includes guideposts for vendor management, and is in fact explicitly intended to “provide[] a common language to communicate requirements among interdependent stakeholders,” including external

19. Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule* (2006), <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>.

20. See, e.g., Complaint, Nations Title Agency, Inc., FTC File No. 052 3117, No. C-4161, at 4 (F.T.C. June 19, 2006), available at http://www.ftc.gov/sites/default/files/documents/cases/2006/06/0523117nationstitle_complaint.pdf.

service providers.²¹ The NIST Framework targets those organizations within critical infrastructure sectors, but provides a helpful roadmap for any business, advising that cybersecurity roles and responsibilities for third-party stakeholders be established and understood by those entities, and that all external service provider activity be monitored to detect potential cybersecurity events.²²

STATUS REPORT—WHAT ARE BUSINESSES DOING TODAY?

The problem is not that businesses aren't vetting their vendors at all or that they are completely failing to oversee their activities; the general consensus amongst regulators has been that businesses are not doing *enough*. For example, the NYDFS found that 95% of the banking organizations it surveyed conduct specific information security risk assessments of at least their high-risk vendors, and 95% also have information security requirements for third-party vendors.²³ However, that same survey found that fewer than half of the banks required an on-site assessment of their vendors, and 30% did not require their vendors to notify them in the event of a cybersecurity breach.²⁴ In its examination of fifty-seven registered broker-dealers and forty-nine registered investment advisers, the SEC's OCIE reported similar deficiencies in the area of vendor management in 2015, finding, for example, that only 51% of broker-dealers and

21. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, at § 3.3, available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

22. *Id.* at DE.CM-6, ID.AM-6, PR.AT-3.

23. N.Y. State Dept. of Fin. Servs., *Update on Cyber Security in the Banking Sector: Third Party Service Providers*, at 2–3 (2015), available at http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

24. *Id.* at 3, 5.

13% of advisers maintain policies and procedures related to information security training for vendors authorized to access their networks.²⁵ If organizations in highly regulated sectors are falling short when it comes to vendor management, you can imagine how less regulated organizations may stack up.

In its seminal guidance on this issue, useful for businesses in any industry, the Office of the Comptroller of the Currency (OCC) has observed:

[t]he OCC is concerned that the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships. The OCC has identified instances in which bank management has:

- failed to properly assess and understand the risks and direct and indirect costs involved in third-party relationships.
- failed to perform adequate due diligence and ongoing monitoring of third-party relationships.
- entered into contracts without assessing the adequacy of a third party's risk management practices.
- entered into contracts that incentivize a third party to take risks that are detrimental to the bank or its customers, in order to maximize the third party's revenues.

25. UNITED STATES SECURITIES AND EXCHANGE COMMISSION OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, CYBERSECURITY EXAMINATION SWEEP SUMMARY, at 4 (2015), *available at* <https://www.sec.gov/about/of-fices/ocie/cybersecurity-examination-sweep-summary.pdf>.

- engaged in informal third-party relationships without contracts in place.²⁶

All organizations need a comprehensive vendor management program to address the foregoing ubiquitous concepts. However, regulators also recognize that vendor management cannot follow a one-size-fits-all blueprint. For example, the OCC has advised that “[a] bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.”²⁷ The FTC, which espouses a similar view,²⁸ maintains that its requirements “are designed to be flexible[;] [c]ompanies should implement safeguards appropriate to their own circumstances.”²⁹

So what should you do?

BATTLE PLAN—WHAT SHOULD BUSINESSES DO?

Regardless of the specific legal requirements—or lack thereof—facing your particular business, effective vendor management should be considered a best practice no matter your industry. In the words of the FTC, “safeguarding customer information isn’t just the law. It also makes good business sense.”³⁰

26. OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC BULLETIN 2013-29, available at <http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>.

27. *Id.*

28. A plan to comply with the Safeguards Rule “must be appropriate to the company’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.” Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule* (2006), <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>.

29. *Id.*

30. *Id.*

An effective risk management strategy involves oversight of the vendor throughout the life cycle of the relationship, from due diligence through termination. But, first, a business should conduct an internal risk assessment. Consider: i) taking inventory of where, what kinds, and how much sensitive data lives on and off your company's systems; ii) the access points to your sensitive data; and iii) your company's overall risk appetite. After all, it is hard to appreciate the risk a vendor may present to your data or your systems if you do not have at least a basic understanding of those elements.

Once an internal risk assessment has been performed, your organization will be primed to evaluate vendors. The following considerations, crafted from available regulatory guidance, best practices, and personal experience, cover the most important elements in the vendor management process, though it would be best to make sure you follow all guidance from your primary regulator in this space. This framework can apply equally to the selection and retention of new vendors as well as the review of existing vendors.

Phase 1: Due Diligence

Due diligence in selecting or reviewing vendors should be commensurate with both your organization's risk appetite and the nature of your relationship to the vendor. Consider a tiered approach to vendor management, whereby you categorize each vendor by data security risk to your business. This approach is sometimes referred to as stratification—the placement of vendors with similar risk profiles into tranches of risk. You can then tailor your risk management approach to each tranche. For example, this may inform your thinking about how much cyber liability insurance a vendor may be required to carry.

Below are some action items and considerations when evaluating potential or existing vendors that will help your organization more fully understand the risk presented by a vendor:

- For vendors who will maintain access to your systems, consider the level and frequency of that access (i.e., will they have administrative privileges? If so, they would present a greater security risk).
- For vendors who will be storing or handling sensitive data, consider the type and volume of data you transmit to them.
- Assess the financial soundness and stability of the vendor by reviewing audited financial statements.
- Determine whether the vendor has ever experienced a data breach, and, if so, how the vendor responded and what remedial steps the vendor has taken to prevent a similar breach.
- Request data security customer complaints filed against the vendor.
- Investigate previous data security regulatory enforcement actions and civil litigations.
- Review the vendor's web sites and other marketing materials to assess the adequacy of the vendor's representations regarding data security and privacy.
- Determine whether the vendor has cyber insurance, and, if so, ask to review a copy of the policy. In particular, examine how the sub-limits are structured.
- Evaluate the vendor's information security and incident response programs, including whether they contain the safeguards to protect personal

information you would expect, and how frequently these programs are reviewed and updated.

- Consider the lack of a formal information security program and/or incident response program as a red flag that the vendor is ill-prepared to provide adequate data security.
- Ask for results from the most recent independent security assessment of the vendor, and any documented remediation actions that resulted from the assessment.
 - If available, review Service Organization Control (SOC) reports and any certification for compliance with internal control standards, such as those promulgated by NIST and the International Standards Organization (ISO).
- Ascertain the extent to which the vendor will rely on subcontractors to perform the contemplated services and whether those vendors are storing that information.
- Ask how often employees receive training on data privacy and security.
- Ensure that the vendor conducts thorough background checks on the employees who will have access to your company's sensitive data.
- Consider an on-site visit to the vendor to more fully understand the vendor's operations and capacity.

Phase 2: Contract Negotiation

The traditional template vendor contract must be modified to address the evolving cyber liability landscape. For example, indemnification and limitation of liability language should explicitly address data breaches. Businesses now need to specify what dedicated amount of cyber liability insurance coverage its vendors are expected to carry (and perhaps even the types and amounts of sub-limits that should be maintained). Parties should clearly outline what notification obligations will be discharged following a security incident, to whom, and when.

Those businesses that find themselves in a regulated environment are now able to use the regulatory guidance that demands improved vendor oversight to exact more negotiation leverage. As regulators continue to fashion guidance about what are and are not sound data security practices, the practical effect is that these concepts will be woven into vendor contracts. In other words, the 800-pound gorilla that used to be able to flex its industry muscle to unilaterally dictate major contractual terms may be losing some ground. The stigma of a data breach is certainly helping too. Explicit data security safeguards (physical, administrative, and technical) are appearing with increasing frequency in lieu of a general mandate to follow “industry standards” in order to provide greater accountability. Vendors are being required to undergo audits and other assessments, often at no additional cost to their business partners, to validate the vendor’s data security practices. These have become new contractual norms, in part due to heightened regulatory scrutiny surrounding vendor management.

Here are some particular contract points to consider:

- Clearly define the types of personally identifiable information or other sensitive data that will govern the vendor’s contractual obligations.

- Specify the data security safeguards (e.g., encryption, intrusion detection and prevention systems, firewalls, data segregation) that you expect the vendor to utilize.
- Require compliance with applicable data security and data breach notification laws and regulations.
- Require the vendor to notify you immediately if a data breach is suspected.
- Require that the vendor preserve all logs, files, and documents related to any suspected breach.
- Require the vendor to conduct an internal investigation if it suspects a data breach, and/or to cooperate with any investigation by your organization.
- Clearly establish which party bears the responsibility of notification to any customers impacted by a data breach.
- Require the vendor to conduct regular audits and submit reports to your organization.
 - Include the types and frequency of audit reports your organization is entitled to receive from the vendor (e.g., financial, SSAE 16/SOC 1, SOC 2, and SOC 3 reports, and security reviews).
- Retain your organization's right to conduct its own audits of the vendor, or to engage an independent party to perform such audits.
- Consider requiring the vendor to carry cyber insurance, as well as naming your business as an additional insured.
 - The case law is still evolving on this topic, but a general commercial policy will likely not

cover your business in the event of a data breach by a vendor.

- Memorialize background check and training requirements.
- Establish what role subcontractors will have in the performance of the vendor's services, including access to and storage of sensitive data.
- Include an indemnification provision that would require the vendor to fully defend, indemnify, and hold your organization harmless from any and all third-party claims, first-party losses (which should be defined to include data security incident investigation costs and customer and regulatory notification costs), expenses, and reasonable attorneys' fees that it should incur in the event that the vendor (or one of its subcontractors) sustains a data breach.
- Try to eliminate any limitation of liability that puts a cap on the amount of damages the vendor would have to pay if it sustains a data breach (or at least an exception to the cap if the vendor fails to meet legally, contractually mandated, or industry standard data security requirements).
- Provide for termination of the contract if the vendor fails to implement and maintain sufficient data security practices, and/or if the vendor sustains a data breach.
- Require secure disposal of all of your company's sensitive information maintained by the vendor following the conclusion of the business relationship.

Vendor relationships are often the product of multiyear contracts which must typically come up for renewal before new language and requirements can be negotiated. But consider asking for contractual amendments or addendums that speak to these measures now if your organization has the leverage to do so. It is worth noting that some cyber liability policies require the insured to establish that its in-house or outside counsel has reviewed the governing vendor agreement in order to provide coverage for a data breach that is the byproduct of the vendor's acts or omissions.

Further, the contract negotiation process is an excellent way to conduct further due diligence. If you want to see where a vendor may be weak, pay attention to the contractual provisions it pushes back on.

Phase 3: Monitoring

As with the other phases of vendor management, the nature of any ongoing monitoring should align with the risk profile of the vendor. More extensive monitoring may be necessary for those vendors who pose the greatest risk to your organization. If resources allow, it would be beneficial to have dedicated personnel at your organization responsible for monitoring and periodically evaluating the vendor's data security practices. You could also engage an independent consultant to perform this task. Generally speaking, monitoring should mirror the due diligence actions set forth above. Specifically, you should also consider the following:

- Restrict and monitor the vendor's access to your company's systems—allow only as much access as the vendor needs to complete the services provided by the governing contract.

- Consider putting on a security training program for the vendor's employees who will be accessing your company's systems.
- Ensure that the vendor conducts its own ongoing data security training of its employees.
- Ensure that any access credentials provided to the vendor are not being misused or provided to unauthorized persons.
- Conduct regular on-site data security inspections and audits according to the type and frequency set out in the governing contract.
- Ensure that any data security issues that arise during inspections, audits, or otherwise are properly addressed by the vendor.
- Watch out for any customer complaints, regulatory investigations/enforcement actions, or civil litigation brought against the vendor, even if unrelated to your organization or industry.
- Establish that access, use, and/or storage of your sensitive data has been discontinued following termination of the business relationship. Receive written assurances that your sensitive data has been purged.

CONCLUSION

In an environment where the term “data breach” has entered mainstream media and executive management is being sued for failure to give proper oversight to company cybersecurity practices,³¹ no business, no matter the size, can afford to ignore or minimize the risk that its vendors present. One analyst writing for *Forbes* described a “Cybersecurity Domino Effect”:

31. See, e.g., Complaint, Palkon v. Holmes, Civ. Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014).

Here's the fundamental truth: We can no longer worry only about our own organization's network security, because so many networks are interconnected and interdependent. A breach in one can easily affect every company in a supply and delivery chain. In fact, we may only be as secure as the least secure partner with whom we connect.³²

Don't let one of your vendors be the weak link in the chain.

32. Ray Rothrock, *Why the Cybersecurity Domino Effect Matters*, FORBES (May 18, 2015, 10:00 AM), <http://www.forbes.com/sites/frontline/2015/05/18/why-the-cybersecurity-domino-effect-matters/#eecad607ee45>.



**MOVING THE LAW FORWARD
IN A REASONED & JUST WAY**

Copyright 2016, The Sedona Conference
All Rights Reserved.
Visit www.thesedonaconference.org