ETAC Cybersecurity Principles

Financial Innovation Lab

Idaho Department
of Finance

The Emerging Technology Advisory Council (ETAC) serves the Idaho Department of Finance (Department) strictly in an advisory capacity. As such, the views and opinions expressed in this report represent those of the ETAC only. The Department does not endorse this material and makes no representation regarding the accuracy or completeness of its content.

To view more information about the Emerging Technology Advisory Committee, visit finance.idaho.gov/securities-bureau/financial-innovation-lab/

Table of Contents

Financial Innovation Lab Mission

1. We are committed to the protection of Idaho’s “at risk” populations (such as our seniors and children) through ethical practices and the judicious use of technology, ensuring a sure and trustworthy financial environment.
2. The Financial Innovation Lab’s core principle is the protection of Idaho’s “at risk” populations from exploitation through the collaborative efforts of state, federal agencies, and private industry. We are dedicated to safeguarding their financial and mental well-being and fostering a secure investment environment.
3. At our core, we embrace technology to innovate and enhance all operations, with a steadfast commitment to protecting Idaho’s most vulnerable “at risk” populations. Our approach ensures efficiency, adaptability, and a forward-thinking stance, achieved through the collaborative efforts of State / Federal Agencies & private industry.

Cybersecurity Principles

principle (noun) - a ***fundamental truth*** *or proposition that serves as the* ***foundation for a system*** *of belief or behavior or for a chain of reasoning.*

The initial set of cybersecurity principles, first developed in the 20th century, has served us well. However, as we quickly approach our first quarter of the 21st century, there is now a need to re-examine these principles and ensure they reflect new cybersecurity risks to organizations. The need also exists for us to look at cybersecurity principles from multiple perspectives, especially in light of an ever-expanding adversarial landscape. In developing these principles of cybersecurity, we consider three such angles in this document:

1. Fundamental aspects of cybersecurity for practitioners and leaders (What should people be doing to ensure cybersecurity success?)
2. Regulatory and compliance efforts impacting organizations (What regulatory / compliance processes work most effectively for organizations?)
3. Technologies and approaches that enable modern marketplace resilience (What technologies will support organizations in the coming years/decades?)

People

Our first set of principles involve aspects related to the people and culture dynamic of cybersecurity programs. The suggested principles build upon a common body of knowledge that all practitioners and cyber security leaders should consider implementing and understanding. These principles serve as both a reminder and as a way to help advance the need to protect against newer methods and approaches by cyber criminals and nation states.

1. Cybersecurity must follow the business, not the other way around

This must be recognized as cybersecurity's first principle. As a profession, we commonly default to "secure things first, do business second." The result of this legacy approach has been the identification of cybersecurity as an obstacle that slows down progress. The legacy approach has a fundamental flaw. Namely, that in order to have things to secure, the business must be in a position to transact goods and services within established markets. Instead, security professionals must remember that our organizations must function and that we, whenever possible, need to create solutions that enable versus hinder the progress of the organizations we support.

2. Integrate cybersecurity into the fabric of the organization, including its processes and technologies, and culture

Cybersecurity as an "add on" has proven its limited efficacy and is inefficient both in terms of dollars spent and time to implement. Instead, we propose that weaving security into ongoing processes and operational controls makes the integration seamless and more effective. This means working with organizational leadership to understand assets, processes, and culture, not just technology. However, cybersecurity leaders must recognize that examinations of this type are not easy tasks to accomplish and additional training and time may be required to achieve this. Training on corporate cultural understanding should be included as a component of program training.

3. Cybersecurity programs need to embrace functional, efficient, and simple solutions

Complex and cumbersome solutions will be viewed as an impediment to the business and people will seek to find ways around complex solutions versus embracing them. Despite education and training, if a cybersecurity program is too complex users will move to avoid active participation. As part of designing a program and its associated controls, a focus needs to be placed on efficiency and simplicity, and preferably transparency, while limiting any process disruption.

4. Compliance[1] does not equal security

We build secure infrastructures and programs that are compliant, not compliant infrastructures that (we hope) are secure. Often, organizations start their journey towards a maturing cybersecurity posture by leveraging compliance as the "first driver." No doubt, any forward progress in enabling a maturing program should be considered positive. While leveraging compliance as an initial step, business and cybersecurity leaders need to develop roadmaps and commit to moving beyond an "only achieving compliance" approach to cybersecurity. Focusing on compliance can, in most cases, improve your security posture (something is better than nothing, as they say) but it is a mistake to equate compliance with security. Two reasons for this:

a. Compliance doesn't take into account your organization's risk posture and may not effectively address holistic risk issues within the organization. In fact, as we outline in the next section, compliance for compliance sake is budgetarily impactful and often leads to over-engineered implementations. A classic example is how organizations handle the Payment Card Industry Data Security Standard (PCI-DSS) which addresses credit card data, but doesn't address other Personal Identifiable Information (PII) examples like Social Security Numbers, addresses, and other contact information.
b. Compliance, ultimately, is not the decision of the cybersecurity professional. Instead, it is a decision that is a determination of whether or not the state of the organization is "legally sufficient" to meet / defend the organization's interpretation of the law/regulation. Legal sufficiency is the bailiwick of the organization's general consul, not the cybersecurity team.

In short, approaching the development and implementation of a resilient and dynamic cybersecurity program that is well aligned to organization risk, secures an environment in alignment with compliance and regulatory requirements.

5. Cybersecurity teams manage risks, and should not build unicorns

Fundamental business logic accepts risks each and every day. Any attempt to create an environment where risk is eliminated is as non-functional as any mythical creature and will break any organization. Absolute security is an oxymoron, while effective security must be a continuous goal. We cannot guarantee that "bad

[1] NOTE: Compliance means to conform to a rule, such as a specification, policy, standard or law.

things” will not occur; we can only minimize both the probability of their occurrence and the impacts associated with those “bad things.” In order to do this, we must embrace a quantifiable and active risk management process that is easily implemented and understood.

Process (Regulation)

The second set of principles considers regulatory and foundational compliance elements that oftentimes are mistaken as the "core" need for cyber security. In our ever-connected world, the need for appropriate regulation and compliance certainly makes sense, but these have to be considered from a pragmatic lens. Instead, businesses are impacted by regulations and compliance requirements that puts aside size (and associated size of risk) and instead require adherence to a "least common denominator" approach. Adhering to cybersecurity regulations pose challenges for organizations of all sizes, but especially for smaller businesses and medium enterprises operating in complex business environments (e.g., the Fintech industry). We recommend the adoption of the key principles presented below in developing regulations, or building cybersecurity programs that align with regulations.

1. One size does not fit all

Regulators should consider that not all businesses are created equal and taking "one size must fit all" approaches create undue burden for larger portions of the market. The burden of proof associated with a breach of the same size and impact is far more impactful to a small business versus its larger market counterpart. Yet, regulatory frameworks – which often prescribe the depth and breadth of control required to achieve compliance – yield stronger alignment to larger, more complex organizations. Regulatory bodies should consider the size and complexity of an environment, such as with the Payment Card Industry Data Security Standard (PCI DSS), and build regulations appropriate to the size and complexity of the environment.

2. Consider business resource impacts to achieve compliance

Just as in the last section where we presented that compliance does not equal security, we now focus on the impacts of budgetary limitations and resource constraints caused by regulatory and compliance requirements. Small businesses in particular may not have the financial resources to hire dedicated cybersecurity personnel or purchase expensive solutions, making it difficult to implement comprehensive security measures. Often, even with resources, finding qualified cybersecurity professionals can be challenging, leaving organizations without the necessary knowledge and skills to navigate complex regulations and implement effective controls.

3. Require clear and concise guidance

Regulatory language is often ambiguous or open to interpretation. This leads to confusion about what steps are actually required for compliance. Further, government agencies and other regulatory bodies may not always provide clear guidance or support for navigating compliance requirements, leaving organizations on their own to interpret and implement regulations effectively. This creates opportunities for internal conflict between cybersecurity and business leadership, enhancing the previous perspective that cybersecurity is the organization's "No!" team.

If regulators were to implement requirements found in prior federal Executive Orders –specifically E.O. 12866[2], E.O. 12988[3], and E.O. 13563[4] – as a core tenant for cybersecurity regulations, and account for the other suggestions in this section, we believe relevant, pragmatic regulations could be better aligned with market size and complexity and would be better understood for businesses to implement.

4. Aligning requirements and eliminating the patchwork quilt of regulations

Organizations often need to comply with a patchwork of regulations from different regions, industries, and governing bodies. Keeping track of these constantly evolving regulations and their overlapping requirements can be a major headache. This is especially true in the area of US data privacy where – without the establishment of a federal standard – businesses are often left a quandary of complex notification rules and possible fines when a data breach occurs. Some regulations may actually require collecting and storing of data, which raises concerns for customers and requires careful balance against other cybersecurity and privacy needs.

Instead, we strongly suggest an alignment of regulatory bodies towards a "common data security and privacy framework" that eliminates conflict of what, when, and for how long to collect conforming evidentiary details. Governmental and regulatory bodies need to define needed regulations and expectations to be crisp and concise so that efforts are aligned, and what gets reported is consistent across all impacted organizations.

[2] https://www.archives.gov/files/federal-register/executive-orders/pdf/12866.pdf
[3] https://www.govinfo.gov/content/pkg/FR-1996-02-07/pdf/96-2755.pdf
[4] https://www.govinfo.gov/content/pkg/FR-2011-01-21/pdf/2011-1385.pdf

Technology

The final set of principles leans forward to present technologies and approaches the cybersecurity profession needs to embrace and move forward with market speed in adjusting to, and adopting to better enable risk mitigation against new threat actors.

1. Data centric security

As public cloud transformations and Software as a Service (SaaS) platforms increase in proliferation, reductions in traditional technology infrastructure (servers, dedicated data centers, etc) is a natural outcome. This leaves traditional business leaders in a position to re-examine what is "most important" to their organization, clients, and partners. We propose that traditional infrastructure - servers, networks, even facilities - will decline in importance as a result of this analysis. Instead, (relevant) data will rise in importance and technologies, frameworks, and entire protection-focused landscapes will change. Understanding key business data flows, storage, and retention controls must take center stage.

Overall, a data-centric cybersecurity program offers a holistic approach to data protection that goes beyond just compliance. It can significantly enhance your organization's security posture, optimize data usage, and drive more effective business outcomes. It's important to note that implementing a data-centric cybersecurity program requires careful planning. We suggest a "measure twice, cut once" model to understanding the technology investment requirements. However, the long-term benefits in terms of data security, business insights, and operational efficiency may make this a positive investment for any organization that takes data protection seriously.

> NOTE: End-to-End Security – Full Lifecycle Protection: Ensuring secure lifecycle management of data, meaning that personal data is securely managed from the moment of collection to the end of its lifecycle. This implies strong security measures throughout the data cycle, including its final deletion.

2. Borderless Identity

Robust cybersecurity requires a reduced attack surface and verified identities. Every organization should embrace strong identity management as a defining principle. We propose the implementation of strong, verified identity management services for organizations to leverage in determining not only who, but when, how, and to what level a requestor should be enabled. Identities must include personas that accurately reflect valid “users” of platforms (e.g. physical users, trust enablement (service) accounts, and artificial personas).

3. Privacy by Design

Privacy, cybersecurity’s equally critical twin, should be integrated into the design and operations of products, services, technologies, and business practices. Privacy by design traditionally includes critical elements such as:

- Proactive not Reactive; Preventative, not Remedial. Promoting, anticipating, and preventing privacy-invasive events before they occur rather than waiting to address privacy breaches after they happen;
- Privacy by default: Ensuring that personal data is automatically protected in any technology platform or business practice without requiring the individual to take any specific action to protect their privacy;
- Privacy Embedded into Design: Integrating privacy into the design and architecture of technology platforms and business practices rather than being an add-on or an afterthought;
- Full Functionality: Encouraging the design of systems that fulfill all legitimate objectives – including privacy, without sacrificing one for the other. This is often referred to as a "win-win" approach or a "positive-sum" game, as opposed to a "zero-sum" game where the gain of one objective results in the loss of another;
- Visibility and Transparency – Keep it Open: Stakeholders, including the individuals whose data is collected, should be able to verify that personal data is processed according to the declared practices

4. Embracing Artificial Intelligence for cybersecurity program support

While the long-term impacts of recent public artificial intelligence (AI) platform releases have not fully been realized, AI is a powerful tool with tremendous potential to revolutionize cybersecurity. By addressing the challenges and implementing AI responsibly, organizations can significantly enhance their security posture, improve defense capabilities, and gain valuable insights to navigate the complex and ever-evolving threat landscape. Leveraging purposeful AI enabled use cases to provide workflow support, automation, and impacts producing positive results.

5. Embed resiliency for continuity of operations

Embedding resiliency into technology platforms delivers a holistic set of benefits, including improved reliability, security, and adaptability in today's demanding and ever-evolving threat landscapes. Resiliency empowers organizations to operate with confidence and minimize disruptions. However, resiliency is not a one-time achievement or a single platform, but an ongoing process that requires analysis and adjustments. Constant vigilance, regular testing, and continuous improvement are crucial to maintain a high level of platform resiliency and reap the long-term benefits it offers.

Resilient platforms can withstand disruptions and failures by utilizing redundancy, fault tolerance, and automated recovery mechanisms. This minimizes downtime and ensures that platforms remain available and operational even when individual components experience issues. Customers and users rely on consistently available and performant platforms. By reducing disruptions, customer / user confidence and satisfaction is boosted, along with overall platform adoption and usage.

The ETAC serves the Idaho Department of Finance (Department) strictly in an advisory capacity. As such, the views and opinions expressed in this report represent those of the ETAC only. The Department does not endorse this material and makes no representation regarding the accuracy or completeness of its content.

To view more information about the Emerging Technology Advisory Committee, visit:
finance.idaho.gov/securities-bureau/financial-innovation-lab/