Digital Trust for banking in the age of insecurity

Matt Konwiser
Cybersecurity Technical Leader
IBM

Christopher Liccardi
Information Security
Federal Reserve Bank of New York

DISCLAIMER:
The views that Chris Liccardi expresses are his own and do not necessarily represent those of the Federal Reserve Bank of New York or the Federal Reserve System.
Many years ago, I worked with someone in marketing who said, “You can make many deposits in the bank of emotion, but only one withdrawal.”

While this holds true for all personal matters, it is equally accurate and much more relevant for financial institutions. Digital Trust is the collection of attributes that create the emotional connection between client and bank as a set of information technology and business values. It takes understanding and preservation of all the values to maintain the Digital Trust relationship. If only it were that simple.

Every day, new online banking capabilities are offered to people and businesses which increase the attack surface of the bank and their clients. Every day, the IT and fraud teams of financial institutions come to work to prevent the bad guys from hitting their target.

Emotional trust is a set of interconnected truths given to us by those we don’t know, but somehow have built a relationship with over time. This trust is something fragile, living and always in need of care. But, for many of us, trust is implicit even in the face of some of the largest data breaches both inside and outside the world of banking and finance.

With the advent of newer, more advanced ways to do less, have we given too much trust to the corporations who handle and manage our money and personal information and asked too little in return? Have we become too disconnected? In light of such a personal relationship is there something we can do to truly earn that trust?

Chris Liccardi
Information Security
Federal Reserve Bank of New York
Contents

Preface 03
Introduction 06
The vendor’s perspective 06
The professional’s perspective 08
Part 1: Motivations 10
Part 2: Best practices 13
Part 3: Business ethics 18
Part 4: The pledge 20
Conclusions 22
The vendor’s perspective 22
The professional’s perspective 22
Final thoughts 23
Digital trust can be largely regarded as a business or marketing problem to solve. While this may be true, there is still an underlying belief that the IT infrastructure of the business, its products, and the connections it has with its clients and partners, are fundamentally secure. If that belief is not upheld, the damage can be severe. IT security is the foundation and if the foundation crumbles it doesn’t matter how solidly the rest of the structure was built.
The vendor’s perspective:

Most security teams are used to dealing with traditional threat/response scenarios. A bulletin comes in saying there’s a new vulnerability or potential attack vector and the team configures their systems to apply patches, check for infections, and filter traffic to prevent anything bad from getting in or out. There is almost no human perspective. In addition, many banks are so large and complex that “right tool for the job” can be replaced by “adequate tool for the job” and the focus is on holding up to audits as opposed to innovations in security.

Introducing Digital Trust to this equation is disruptive, perhaps more so than any other concept to date because it is subjective to the beneficiary of the trust; the financial client. What makes a person or business feel comfortable (or uneasy) may not impact others the same way. These irritants are also dynamic, they change by mood, industry landscape, and geopolitical factors.

Digital Trust can be largely regarded as a business or marketing problem to solve. While this may be true, there is still an underlying belief that the IT infrastructure of the business, its products, and the connections it has with its clients and partners, are fundamentally secure. If that belief is not upheld, the damage can be severe. IT security is the foundation and if the foundation crumbles it doesn’t matter how solidly the rest of the structure was built.

The biggest hurdle for the financial sector is that they are heavily regulated, and it’s easy to say that regulatory compliance and audit is at the top of the priority list because it’s known and addressable. That is exactly the problem. Digital Trust is not regulated. It’s an idea, and ideas can’t be manifested in the form of a spreadsheet or checklist.
There is no lapse or failure in detection or response that doesn’t in some way have a very real human impact.

To address business risk, security teams must regard themselves as safety teams. Safety has a personal connotation. A safety team looks out for people. They walk employees to cars. They monitor surveillance cameras at entrances, elevators and hallways. They use situational awareness, behaviors and instinct to identify potential threats. No safety team ever said “Well, two people were murdered but at least now we know there’s a murderer out there so we’ll be more careful next time.” They’ve also never applauded their ability to patch a stab wound when they missed the fact that the attacker gotten past them in the first place.

Digital trust requires digital safety. The way IT security teams align to the premise of digital safety is to think differently. When a security team at a financial institution is unsuccessful at their task, the head of a household can’t pay their rent. A professional driver isn’t covered when another driver hits them. A student can’t get their first credit card. A business can’t make payroll.

While this philosophy for IT security has many gray areas, there are also many opportunities to shine. At a public speaking engagement at a university, General Michael Hayden, a former director of the CIA, said this: “Most of the things we need for cybersecurity are within the reach of American business.”

This can be interpreted simply: the capabilities exist—we just need to deploy and use them in a way that aligns with the nature of the threat and the needs of the clients.
The professional’s perspective:

Trust is a human concept. Digital trust is that same concept, applied in a technical measure to ensure something we feel is, in fact, something we can count on.

The adage, “if it’s not one thing, it’s another” fits well within the corpus of security in any organization that strives to be security aware. That awareness doesn’t even have to take into consideration a lack of focus on security innovations to be effective or relevant.

This best effort mentality keeps us out of trouble within the Audit and Compliance frameworks, but never really gets to the heart of Digital Trust. Often, we know we’re missing the point; that point being that trust is something that takes effort and work, even if that work is inconvenient or uncomfortable.

In the “catch as catch can” world of digital security, we assume a great deal, especially when it comes to our own security in the hands of people that we’ve never met. This can be proven simply by asking yourself how many people, from any breach you’ve been involved in, actually picked up the phone and called you to ask how you were doing since that breach. I venture a guess that number is less than you’d hope.
Organizations such as banks, insurance companies and any others that handle vast amounts of personally identifiable information (PII) know where the line between “good” and “good enough” is drawn. Do they have the power to address the “good enough” in a fashion that builds trust or are they phoning it in?

Examining many different cases can prove that the technical capabilities exist to further digital trust, but often outside factors are at play that prevent those innovations. Trust is a human concept. Digital trust is that same concept, applied in a technical measure to ensure something we feel is, in fact, something we can count on.

Security bullpens are full of teams, busy with the theoretical and the practical but lack the buy-in to take it to the next level. Is it a matter of budget or just ignorance of how far security needs to function in order to build that bridge between technical capabilities and the business objective of trust between company and consumer? The idea of trust itself is, on its own merits, something we want to count on and while its strongest argument is its strength and endurance once given, it is also its weakest link. We trust implicitly in things we believe in, but do we ever utter the words “prove it” to the those who could lose that trust so completely?

While these perspectives may seem esoteric or philosophical rather than programmatic, there are four areas that an IT security team can focus on to help establish and preserve Digital trust.
Part 1: Motivations

For defenders and attackers, understanding what drives someone is critically important. If the people out there who are protecting the world love their jobs, believe in what they’re doing, and know the positive they are contributing, they will simply be better at it.

This goes to “finding the why.”

Conversely, the bad guys are also highly motivated. Driven by personal, political or financial reasons, they are attempting to inflict as much damage as they know how to cause.

In most cyber investigations, a “why” could be:
- We didn’t patch our systems in time (or at all).
- Someone mis-configured a firewall.
- There was a rogue application.

In a Digital Trust investigation, a “why” should be:
- The suspect’s parent lost all of their money in the stock market and they conspired with known hackers to infiltrate and steal.
- The suspect didn’t get the promotion they wanted, and in retaliation planted malware on the network to cause general havoc.
- The client’s account was compromised and after a complex social engineering effort and coercion campaign, a client, their relationship manager and a third party conspired to defraud.
The leadership team should work against KPIs that focus on unity, agility, innovation, and success measures that build and preserve the organization’s client’s digital trust, not myopic information technology or security specific goals.

Hopefully, the differences in these are evident. From the perspective of Digital Trust, “why” should be relative to the individuals or businesses involved and impacted, not the IT elements that were impacted. This is the only way possible to isolate cause, effect, damage and attempt to execute a complete remediation. It is also the only way you can learn from the event and find it faster should it happen again.

The business can also learn from the “why”—are there better ways to support employees and clients to contain negative sentiment? Are there ways to monitor overall sentiment and use rapid or uncharacteristic changes as a form of threat precognition?

For this flow to work, the social media, HR and customer satisfaction teams must be trained in the basics of cybersecurity and there must be pre-planned procedural materials instructing those teams and the IT security team how to handle an event when it appears on the radar.

The leadership team should work against KPIs that focus on unity, agility, innovation, and success measures that build and preserve the organization’s client’s digital trust, not myopic information technology or security specific goals.
The front-line teams should always keep the beneficiary of their success in mind; the individual or business who needs their assets protected.

To understand how important every element of the Digital Trust chain is, you need look no further than the game of Tic–Tac–Toe.

It’s a very simple game; 9 squares, two options (“X” or “O”). It is also impossible to win or lose if both sides are paying attention. With a limited number of possible moves, it’s very easy to see where you need to take the next action, yet people still win (and lose). This happens because they lack the motivation to keep playing.

In security, every minute of every day we play Tic–Tac–Toe in an endless loop. We will never win, but we should never lose, and as soon as we stalemate our opponent, the game starts over. It takes the right people with the right motivation to keep playing.

If a bad actor loses, they risk their reputation and they don’t profit. If the security team loses, they risk the Digital Trust established between their company and every one of its clients. Recent events have also shown that the impact of these losses is starting to have massive implications for the careers of executives and senior leadership teams.

The analogy may be simple but the process of picking the next square for your “X” is anything but. Highly motivated teams cannot summon decisions out of thin air, using divination or a crystal ball. They must follow a set of best practices that integrate the well–known anchor tenants of people, process, and technology to allow them to force the stalemate.

These best practices should also be oriented towards creating waves of noise for the bad actor, setting up a barrier of obscurity and complicating their next move as well. Endowing teams with these capabilities also feeds the motivation to succeed; after all, the one with the coolest toys wins.

The most important factor though, is that senior leadership sets a tone and tenor, and builds a culture that focuses not merely on compliance, but on building and preserving digital trust as the core business asset to be protected.
Part 2: Best practices

This can easily be the most painful part of the conversation for myriad reasons:
- It means spending money.
- It involves change.
- It uncovers your weaknesses and gaps.
- It forces you to make logical, not emotional decisions.

It’s also the only thing standing between a highly motivated security operations team and their ability to take down a bad actor.

Best practice domains for a Digital Trust security are represented with this simple illustration:

---

Security Operations includes endpoint and server management, network infrastructure, application development and testing, data protection, identity/access management and governance, and security operations center functions.
The challenge for banks, of course, is to capture the business of the tech-loving crowd while continuing to serve the older, more affluent customers in a cost-effective manner.

Every financial services organization has portions of this framework in production—it’s required by regulation to operate in the United States. Only a few organizations have figured out how to orchestrate the actions within and between these domains. Even fewer still can investigate any incident as a compound business problem as opposed to an isolated incident.

There is no simple bridge to get from learning about a Digital Trust security framework to adopting it. Many hurdles exist based on how organizations operate today. Some hurdles will slow adoption, and others can endanger their ability to preserve the Digital Trust foundation. The below are some of the most common ways organizations can hinder the process:

- “Adequate tool for the job”: Organizations that reuse capabilities implemented for one purpose to handle another. They do a good enough job to pass a compliance checklist, run a query, or even assist with an isolated investigation but they cannot support proactive detection or create a seamless security posture.

- “Not invented here”: Only in the past five years have tools matured to a point where regulated organizations can use them nearly out of the box. This forced many regulated businesses to develop their own tools. Now, the home-grown tools are heavily integrated to the business but are a budget black hole and too painful to displace. As a result, they’re left in place for regulatory or basic investigational needs and significant investments are routinely made for upkeep—but for most organizations, it’s impossible to keep current with the new threats with a home-grown solution.

Fraud focuses on the transaction data including wire, online, teller initiated, third party brokered, Blockchain, and policy and claims anomalies.

Incident Response incorporates governance, compliance, audit, and runbook activities providing protocols to follow in the event of an incident.

Investigation is a fusion center style operation that can access information and incidents from all three subordinate domains plus access critical personnel and corporate records to create a complete picture of events, history, associations, impacts and event relationships.

Each of the three subordinate domains have their own process lifecycle including baselining, management, detection and remediation. Investigation is only triggered based on an event and has a linear process of data ingestion, correlation, interpretation and output. It operates above and independent of the three, due to its highly-sensitive data and specific need to cross business boundaries.
You must also be prepared to handle the cultural changes required to reposition as a Digital Trust–centric organization.

- “Build a quilt”: Buying tens or hundreds of niche applications from small companies that may be best of breed, cutting edge or just “cool.” Then forming a security posture by attempting to stitch them all together. Often, these are the same organizations who build their own systems or reuse capabilities because they have numerous gaps that need to be addressed and the smaller niche players fill the gaps without overlapping existing capabilities.

- Something here about culture: Lip service to security and trust, while not baking it into every decision that’s made.

No matter the reason, financial services organizations who ended up in one or more of these categories are at risk. If the objective is to protect the business and preserve the Digital Trust relationships, how will not using the right tools for the job, using only home-grown and high OPEX tools, or implementing hundreds of patchworked capabilities support that mission?

Hint: It won’t.

With all this potential friction, the best way to start bringing the teams around is with external influence. Leverage research, consultants, your peers to identify what’s missing, what others are doing, and what has and hasn’t worked.

Next, test your theories. Use war games, external vulnerability testing, and “live fire” scenarios that incorporate the entire organization, not just IT or security, to see how people respond and how quickly you can identify root cause, total exposure, and source motivation.

Third, deploy the new workflow against a recent past incident and see if you can expand your view of what happened or arrive at different conclusions.

Ensure through all of this you are always using data from Security Operations, Fraud, Incident Response and enrichment from other sources for every investigation.

Keep everyone focused on the task at hand—protecting the organization by safeguarding the Digital Trust relationships your company has with its clients.

Lastly, remind everyone of their combined purpose. It isn’t to pass an audit or remedy an ailing endpoint or a corrupted database. It’s to find the underlying bad actors and their motives for doing what they did—the “why”. You can’t fix something if you don’t understand it.

And almost every time, the “why” stems from a business matter.
Part 3: Business ethics

Asking why, often times, why am I here each day in the face of such vast security adversity, is almost always an internally directed question. It isn’t one that is asked aloud with an expectation of an answer nor is it a question a security team’s members ask each other. When I started my career in security and technology so many years ago, one of my professors began a class by stating the following; “so you want to be a dentist.” Odd to say the least and it took many years in practice to determine his sarcasm did have a point. This job ain’t easy folks – it never will be.

The discussion of ethics usually revolves around the traditional topics of business ethics as they relate to business practice and principle. Organizations even go as far as erecting a set of ‘ethical walls’ to establish the appearance of not sharing data or practices between competitors within the same vertical. That level of ethical compliance is easy to implement and easier still to measure. We can “check the box” for this round and feel confident we accomplished this task.

Seldom does the discussion of ethics focus inward on security; more to the point, do the ethics of security entail asking questions of whether what we’re doing makes the most sense when it comes to our customers and their digital trust? How many of us have sat in meetings discussing things like ethical practice in theory only to wander, bleary-eyed, into our next meeting where we discuss a lack of control on some rogue security facet that may never get addressed?
When it comes to digital trust, a more apt question should be what am I doing to enhance and deserve the trust given to me by my organization’s customers? The natural inward progression of those interrogatives may follow; what are we doing to ensure our customers data is safe each and every day and how am I making that happen? Answering those honestly may shed a little light on the bigger question of Digital Trust.

While traditional definitions of business ethics include such vague gems as “code of behavior” and “corporate responsibility”, rarely do they ever get applied to ourselves in terms of what a security professional or a security team is doing to build and maintain that trust. Are we so focused on maintaining a culture of check-box adoration that we miss that bigger picture of how does our own schedule shape our need to get things done even when those things are transactional and not of greater value to the customer? My approach is more critical; what are we not doing to earn that trust? How am I taking that trust to heart and building on it to make sure I never lose it? Security professionals should propel security forward and not become roadblock or an obstruction to digital trust.

Ethical concerns need to become a guidepost for digital trust, and must flow from the board down. Those ethical concerns need to come in the form of security staff asking how are we building trust with our consumers? How are we stepping beyond the technical and moving directly into the personal to enhance that trust? Answering questions similar to those takes a step toward solid foundations in digital trust.
What it comes down to is a pledge. A pledge to build, maintain and defend the trust given to me by consumers who believe I will strive to make a difference, even if they don’t realize it.

When it comes to digital trust, a more apt question should be what am I doing to enhance and deserve the trust given to me by my organization’s customers? Security is not just a collection of technologies that come together to paint a picture or display a set of alerts on a screen; it is a way of life. As with other aspect of life, the more personal you make it, the better the return you get on your investment. Considering how much time we spend at work, that investment can mean the difference between good and merely good enough.

As I set writing this, I am reminded of the challenges I’ve faced just proving my security voice is worth hearing. Not just fighting for the next great paycheck, but also fighting for something I believe in. I am reminded of the pledge I had to take when I acquired my security certification. In short it comes down to this; I work each day to protect the common good, society and public trust... and the fact that it reads like a super-hero oath hasn’t slipped my attention. What it comes down to is a pledge. A pledge to build, maintain and defend the trust given to me by consumers who believe I will strive to make a difference, even if they don’t realize it.

I tell myself each day, when I begin to look at all the cases and technical challenges I face, that I need to try harder; I can always try harder. As a security practitioner, I need to step outside the reliance on solutions built or unboxed and move closer to the consumers I support, directly or indirectly.
Organizations need to look at the principles and practices we know we should adhere to and beyond the excuses we sometimes know are coming in order to ensure that trust is not misplaced. No monumental project ever undertaken was looked at in the beginning stages as easy. Digital trust is as monumental in commitment as it is in impact to the consumer and the organizations seeking that trust. By working at it each day, by playing tic–tac–toe the right way, we may never actually win; neither will we actually lose.

Another adage that comes up in clichéd conversation when one works in security is the “when, not if” methodology. While often, this old chestnut comes when discussing potential security breaches, insider threat actors and other disruptive forces at play against our businesses, it can also stand for doing security the right way. When we consider the trust given to us, when we decide that more secure, less obscure is better; when we think about the consumer first and the cost of “good enough” second, only then are we striving for trust; true digital trust.
Conclusions

The vendor’s perspective
- Keep the focus on the safety of your clients.
- Remember that bad actors always have a reason for doing what they’re doing.
- Don’t get stuck in the past or hung up on doing things the way they’ve always been done.
- Create a centralized Digital Trust security framework.
- Unify workflow for security operations, fraud, and incident response.
- Investigation process and outcome should always be centered on the “why”.

The professional’s perspective
- Why are we here leads to why aren’t we doing better for our clients?
- Ethics isn’t just for business, it’s a guidepost for being ethical when it comes to trust.
- Trust may be based on “out of sight” but should never be out of mind.
- Digital trust is not a collection of technologies, but a methodology for the consumer.
- Do the right thing isn’t always “do the easy thing” — though we almost always know what the right thing is.
- It’s never just good enough when it comes to trust.
In a regulated business, it’s too easy to focus on compliance and frameworks, and ignore the real reason an information technology team is there; to protect people’s money.

Digital Trust is disruptive. It forces financial institutions to think differently about their mandates and how to handle incidents. It challenges long standing methodologies and behaviors. It forces organizations to change how they measure their team’s successes and failures.

And that is all good for the organization and its clients.

In a regulated business, it’s too easy to focus on compliance and frameworks, and ignore the real reason an information technology team is there; to protect people’s money. Regulations will never keep pace with technology advancements.

Executives must establish KPIs to focus themselves and their teams on protecting digital trust. Technology and process must be continuously overhauled to bring fresh ideas and innovations to the Digital Trust security lifecycle. The front–line experts need to be kept motivated and focused on the task at hand.

Digital Trust security is not another checklist. When teams and their technology and processes adapt they will be well positioned to focus on the “why” every time and detect and manage new attack methods nearly as fast as they can be developed.

How well are you maintaining Digital Trust with your clients? Contact IBM for a comprehensive assessment of your ecosystem, where we will provide actionable feedback for your organization.

Assess your security readiness for digital transformation at ibm.biz/BdYjzp

— Matt Konwiser
Contact IBM to assess your security readiness for digital transformation at ibm.biz/BdYjzp

For more information visit ibm.com/banking