TPX®

# FINANCE INDUSTRY CHEAT SHEET

# inside

click on text to jump to section | click ☰ to return to here

ELEVATOR PITCH 3

GOOD TARGETS 3

FINANCE INDUSTRY OVERVIEW 4

TIPS ON SELLING INTO THE FINANCE INDUSTRY 5

CYBERSECURITY & FINANCE 5

POSITIONING 9

CONVERSATION STARTERS 10

HANDLING OBJECTIONS 10

CHALLENGES & SOLUTIONS 11

# 1 Elevator Pitch

In partnership with TPx, we offer a cost-effective way for financial entities to have a highly specialized IT team on hand to help fight cyber threats, improve their connectivity and collaboration.

# 2 Who is a Good Target?

- Credit unions
- Smaller banks
  - – Harder to attract appropriate talent
  - – More difficult to invest sufficiently in cyber risk security
  - – Easier protection than with larger banks that have more complex/legacy IT infrastructure
- Investment firms and fintech startups
- Tax, accounting, and insurance services

> Cyber attacks pose the most serious threat to US financial institutions and the system as a whole."
>
> *CEOs of four of the nation's largest banks to Congress, May 2021*

## Smaller vs larger financial institutions

- Smaller banks are more impacted by cyber events than medium-sized banks due to the higher number of entities and share in sector revenue
- Larger banks are more likely to have complex and also legacy IT infrastructure compared to smaller banks, which could increase cybersecurity risk if not properly managed

## Personas

- Every state has a banking association. You can sign up to attend the shows. There are three entry points:
  - – IT department
  - – CFO runs IT department
  - – If a larger bank, then chief security officer or risk officer
- A majority of banks employ strong cyber governance practices, with 95% employing a CISO or CSO
  - – Other personas may include CIO, CTO, chief data officer, chief privacy officer, head of IT risk management
- CISOs at financial institutions:
  - – Often report to the CIO
  - – Their roles and responsibilities are being increasingly diluted across the organization
    - …creating transverse roles such as chief data officer, chief privacy officer and head of IT risk management, which often don't report to CISO
    - …creating unnecessary overlaps/frictions within the organization along IT-heavy security processes
  - – Come from a technical background but increasingly need to rely more on broader business acumen and risk management expertise
  - – Need to have the right blend of technical expertise and good communications skills so they can translate that technical know-how into language that resonates with the Board (often a rare skill for CISOs)
  - – Spend an increasing amount of time being held accountable and justifying themselves than having time to actually do the job of securing the organization
  - – Often have to work in a reactive instead of proactive mode, constantly chasing the train of security priorities instead of driving it

- How bank CISOs often feel…what challenges they face:
  - The board generally understands little about cybersecurity and provides limited support to you. You can't answer questions with certainty such as 'Can you guarantee that an Equifax or a CapitalOne type of event will never happen to us?' because an organization can never be 100 percent secure. You are the one responsible for protecting the organization daily, and yet you are the first person to get axed when a major incident happens.

## 3 Finance Industry Overview

- Chief operating and technology officers face demands around regulation, client service, risk management, liquidity, and cost pressures.
- The industry must continue to cut costs, while fighting for market share, pushing innovation, and managing changing needs among employees, who themselves are adjusting to a new "post-Covid" reality.
- Financial services incumbents often have multiple core legacy systems that are complex and expensive to run and maintain but tricky to change. The stress placed on systems caused by spikes in online commerce since the pandemic has shown that many services and integrations added over the years were not implemented with long-term resilience and scalability in mind.
- Typically extremely risk-aware environment, which causes them to lag behind on technology
- The potential damage from an IT system failure to reputation and trust is now more severe than ever and CIOs and CTOs must continue to prioritize effectively managing legacy tech.
- Many banks are being asked to innovate while lowering structural costs and improving capital returns— and many traditional banks are falling behind.
- Best-performing traditional banks now focus more of their tech spend on growth and innovation rather than on maintenance.
- In modern financial services, fast delivery of new digital products and services must be balanced against the security and reliability of the system.

### The industry is heavily influenced by:

- Digital technology/transformation
  - Automation & orchestration
  - AI
  - Customized experiences
  - Digital platforms
  - New operating models and channels
  - Next-generation applications
  - Increased smartphone usage
  - Cloud-based solutions
  - Partner ecosystems
  - 24x7 services

- Stagnating global industry profits
- Growing number of regulations
- Multiplication of audits, reviews and exams when it comes to cybersecurity
  - – Common for internal audit teams to have dedicated human resources focused on cybersecurity
  - – More frameworks are created, and more audits and targeted reviews are performed that increase the stock of cybersecurity findings
- Increased customer-centricity
  - – Customer-centricity has been a winning strategy for fintech firms for some time and is now being prioritized by those who were not already doing so
- Cyber threats [more in next section]
  - – Rising costs of malware and fraud
  - – Hackers are after money and personally identifiable information (PII)

Acquiring and retaining customers in a new digital, multi-channel environment requires innovation and agility. It also requires more robust and intelligent security as both IT and cyber-attacks on financial institutions become more sophisticated.

## 4 Tips on Selling into the Finance Industry

- Typically extremely loyal customers who will come to you for additional help once you've helped and established trust.
- Banks are lucrative due to high-security requirements = larger budget, more resiliency. (SMB banks typically expect a $1K/month investment, vs. a small law firm who expects $300/month security/IT spend)
- Value sell — don't sell on price.
- Longer sales cycles in this industry, so be patient.
- Very close-knit community that is hesitant to take on new vendors: they like to buy what similar entities buy. The best way to get in the door in finance is a referral, VAR, or supplier they trust.
- Hard to crack a shell, but once you do, they talk to other banks. They have private forums and banking IT-focused groups, so you likely get more business this way.

## 5 Cybersecurity and the Finance Industry

### Attractive target because:

- Entrusted with the personally identifiable information (PII) of every customer (i.e. Social Security number, banking details, phone number, email address etc.)., which is valuable on the darknet
- "That's where the money is…"
- Cybercriminals target corporate information that can affect the share price of a company as soon as it becomes public. This information can then be used to digitize insider trading and front-run the market

> Unfortunately, the banking sector is one of the most heavily targeted by cybercriminals. We are always on the alert. We receive all kinds of threats – from basic phishing emails to more sophisticated attacks. Protection is a matter of having multiple layers of defense not just for the corporate network but also for our employees working from home during COVID-19 and for our customers."
>
> *Kamran Meer, CISO,*
> *United Bank Limited (UBL)*

Board engagement key:

- In a survey of CISOs, the most successful cybersecurity programs boasted active involvement from the board and executive leadership team who made cybersecurity a priority and emphasized a cybersecurity culture.

## The role of technology

The financial industry struggles to keep pace with technological innovation. Legacy systems that would be costly to replace, while only an inconvenience to customers, may pose a significant threat to financial institutions. On the other hand, hackers often benefit from new technologies that make it easier to attack legacy systems.

Thanks to the rapid IT changes and rising complexities (cashless payments; mobile apps; electronic payments etc.), cybersecurity is becoming a top challenge. Managing cybersecurity risk ranked as an extremely or very high priority over the coming two years for 87% respondents of a recent Deloitte survey.

The general sense is that the industry is working hard on cybersecurity, but a lot more needs to be done before banks can feel that cybersecurity concerns have been reduced to the same level as physical security concerns.

When banking and fintech systems are suboptimal from a security and operational resilience perspective, the risks to customer trust are substantial if things go wrong. Top of what keeps tech leaders awake at night is the threat of potential cyber attacks.

## Biggest cybersecurity concerns

75% of breaches involve hacking and malware (especially phishing, ransomware and theft of customer data)

18% accidental disclosure

6% insider threats

2% physical breaches

Newer types of ransomware are especially dangerous because they combine the theft of customer data — and extortion — with locking up the victim's networks, forcing operations to shut down.

Spending on cyber security has been growing, although the respondents report finding qualified staff is a big problem. *(Deloitte survey)*

## Managing vendor risk is a critical challenge

Financial institutions rely on a variety of vendors, suppliers, and partners—and those relationships bring increased exposure to the business. They often dependent on third-party solutions that may be antiquated.

$4M According to IBM's Cost of a Data Breach Report 2021, a vulnerability in third-party software was the fourth most frequent source of breaches and cost an average of $4.33 million.

87% of respondents of a recent VMware survey said they were concerned about the security posture of the service providers they rely on (huge increase in "island hopping attacks") – *VMware Bank Heist Report*

## Cybersecurity regulation

In just the last two years, and in addition to existing cybersecurity laws, the financial industry has been saddled with the following regulatory oversight:

- New York State Department of Financial Services Cybersecurity Requirements Regulation for Financial Services Companies Part 500 (NY CRR 500) of Title 23 (including measures that financial institutions needed to take to protect against ransomware attacks)
- US Securities and Exchange Commission (SEC) issued interpretive cybersecurity guidance.
- National Cybersecurity Center of Excellence (NCCoE) released the NIST Cybersecurity Practice Guides SP 1800-5, SP 1800-9, and SP 1800-18.
- 24 states passed bills or resolutions related to cybersecurity

Banks have a 36-hour window for banks to notify regulators of a cyber incident that could materially disrupt operations. Credit unions should have 72-hour time frame under a recent proposal.

As attacks increase, regulators take notice and take measures to increase the pressure on the industry to find solutions. Regulatory and compliance requirements are a significant challenge for the financial sector and the single most important reason that consumers trust the industry with their money.

Cyber-regulation is great for securing budgets and generally helps improve the security postures of organizations. However, it may be perceived as a distraction, because it remains a primarily compliance-driven process: you can “technically” be compliant and still have major unaddressed security risks. Also, the legal and compliance departments want to have a say in everything that the CISO does.

## The Cyber Risk Institute (CRI)

- Launched in May 2020
- Enhances cybersecurity resiliency through standardization
- The financial sector cyber profile tool is the benchmark, which provides a common framework for cybersecurity and resiliency assessment
- Helps financial institutions comply with different regulations and requirements

CYBER RISK INSTITUTE

**90%**

of all financial institutions experienced ransomware attacks

Ransomware attacks have increased by more than 1,318% year over year in the banking industry

The industry is among the top three of the most targeted sectors suffering from such attacks

**1.7x**

Financial services are 1.7 times more likely to be targeted by phishing attacks

*Source: 2021 IBM X-Force Threat Intelligence Index*

## Compelling stats

- The finance and insurance industry sector experienced the **most cyber attacks for the fourth year in a row**. *(2021 IBM X-Force Threat Intelligence Index)*
- Financial gain was the most common motive in data breaches across all industries. In companies with fewer than 1,000 employees, **93% of breaches were financially motivated**. *(Verizon's 2021 Data Breach Investigations Report [DBIR])*
- The financial industry has the **second highest average total cost of a data breach, averaging $5.72M** in 2021 according to IBM's 2021 Cost of a Data Breach report. *(2021 IBM X-Force Threat Intelligence Index)*
- The majority of companies planned a **20 – 30% boost to their cybersecurity budge**t in 2022, primarily into XDR, workload security, mobile security, threat intelligence, and MDR. *(VMware Bank Heist Report)*
- In a recent VMware survey, nearly **3 out of 4 respondents said they'd been hit** by at least one ransomware attack. What's more, **63% ended up paying the ransom**. *(VMware Bank Heist Report)*

## True stories

In the years 2009 through 2019, some of the most recognizable names in this sector were breached on more than one occasion. American Express and SunTrust Bank were breached five times, and Capital One and Discover were breached four times each during this period.

### Phishing

- In 2016, in one of the boldest attacks against a financial institution to date, **hackers used the SWIFT banking network to wire themselves $81 million** after breaching the Bangladesh Central Bank using a series of phishing scams.

### Third-party risk

- Consider the case of data and analytics company Ascension, which serves firms in the financial industry. In 2019, **a misconfigured online server exposed 24 million of its financial and banking documents** dating back more than a decade. The leak came from a vendor the company used. As a result, personally identifiable and financial data of many large financial services companies was exposed.

### Insider threat/third-party threat/firewall misconfiguration

- Capital One suffered one of the biggest data breaches in the industry in 2019, when **106 million records were exposed after a malicious threat actor exploited a firewall misconfiguration**. The hack included every existing customer, every previous customer and anyone who applied for a Capital One card. At the time of the breach, the attacker was employed as a software engineer at Amazon. Capital One's data was hosted on a server rented from Amazon.
- A breach at Flagstar Bank resulted in more than **1.5M customers' social security numbers being stolen**. It was the second to impact the bank in less than two years and it took six months for Flagstar to notify customers.

*Source: Fitch Ratings, Carnegie Endowment for International Peace.*

### Examples of Recent Attacks

| Date | Country | Company | What | Cost | Impact |
|---|---|---|---|---|---|
| 7/20 | US | 'Dave' banking app | Data breach |  | Personal info, encrypted SSNs and hashed passwords of 7.5m users leaked |
| 5/20 | Norway | Norfund | Data breach/theft | USD10m | $10m stolen via a fraudulent loan, likely following business email compromise |
| 3/20 | UK | Finastra | Ransomware attack |  | Partial outage over several days affecting client banks, particularly in North America |
| 12/19 | UK | Travelex | Ransomware attack | GBP25m | Outage of more than a month, cost is an estimate |
| 11/19 | Canada | Desjardins Group | Data breach | CAD108m | All 4.2 mil. member accounts affected |
| 7/19 | US and Canada | Capital One | Data breach | USD145m | Over 100m records affected, cost includes USD80m penalty |
| 5/19 | US | First American Financial Corp. | Data breach |  | 885m files containing personally identifiable information exposed; in Jul 2020 the regulator filed charges seeking penalties |
| 10/17 | Taiwan | Far Eastern International Bank | Theft | USD14m | Via fraudulent SWIFT transactions, with a ransomware attack as a distraction |
| 9/17 | US | Equifax | Data breach | USD700m | 148m accounts affected |
| 11/16 | UK | Tesco Bank | Theft | GBP18.7m | Via vulnerabilities in card issuance processes; GBP16.4m regulatory fine |
| 8/14 | US | JPMorgan Chase | Data breach |  | 83m accounts affected, 1,000 hired for data security |

# 6 Positioning

You are going to be best off putting your foot in the door with SD-WAN or cybersecurity, especially phishing (cybersecurity awareness training, phishing), firewalls, and endpoints (especially MDR) — since these are the industry's top challenges and areas of focus. We stand the best chance for smaller financial entities (refer to "Who is a good target" section).

> "A sophisticated cybersecurity approach to repel attacks should combine remote access, network filtering, and segmentation. And it should be cloud-based including SaaS solutions for capacity and organizational resource availability, simplified infrastructure upgrades, zero-trust defined security measures, and activity monitoring."

### Key positioning statements

- **Cybersecurity + connectivity + collaboration all under one roof**
  You have enough 3rd parties to worry about — minimize the risk and headache by choosing company that can do more for you
- **Trusted partner**
  - Trusted by 1,200 financial customers, we know the industry and its challenges
  - PCI DSS compliant
  - We are big enough to get the job done while small enough to be agile with 18,000 customers across 49,000 locations
  - 120+ certifications across 60+ categories (CompTIA, Cisco, SilverPeak, Fortinet, AWS, SMC and more)
- **TPx has broad cybersecurity services to tackle your pain points**
  From managing your endpoints, monitoring your firewalls in our own SOC, or helping you fight phishing with Managed IDR and cybersecurity awareness training, we can help you tackle your biggest cybersecurity pain points

- **TPx saves you money**
  - – It is often more cost-effective to partner with us than doing it in-house.
  - – Running own SOC is expensive (technology and people to service it 24/7) and many SOCs of financial institutions are overburdened. It often pays off to outsource it. We have our own SOC in Las Vegas with experts monitoring threats 24/7/365.
- **TPx alleviates your staffing issues**
  - – We don't replace your IT team, we augment it, so your staff can focus on business-critical tasks.
  - – If you're having a hard time finding or retaining IT and security staff, partnering with an MSP takes this big pain point off your plate.
- **We let you customize**
  - – Customize your service to best suit your unique needs, we know one size doesn't fit all. What works for a big bank may not work for a small one.
  - – Different service levels, mix and match

## 7 Good Conversation Starters

What are your biggest IT challenges right now?
What are your priorities when it comes to IT?

How are you protecting yourself against cyber threats?
Do you have 2FA?

How do you monitor cyber threats?
Do you have a plan for mitigation?

What is your plan if you get hit with ransomware?

Do you run your own SOC? How is it working for you?

Do you have people working remotely?
If so, how did you adjust your IT?

What plans do you have to digitize your services?

## 8 Handling Common Objections

- **We are too small to be a target.**
  Actually smaller banks are more impacted by cyber events than medium-sized banks. If you have data, you are a target — and cyber adversaries like to zoom in on the low-hanging fruit with limited budgets.
- **We have cyber insurance.**
  While the vast majority of financial institutions have a stand-alone cyber insurance policy, there are gaps and exclusions to such policies. Additionally, most require banks to have a solid foundation in place to be insured. Insurers want to know that there is an organized and proactive effort to manage cybersecurity risk. At a minimum, those measures include:
  - – Multifactor authentication (MFA), backup, incident response plan
  - – Patching
  - – Cyber awareness training for employees

- **We can’t afford it.**
  You can’t afford not to have the core cybersecurity measures in place — and it may be actually a lot cheaper for you to outsource it to TPx than do it in-house. When it comes to cybersecurity, prevention is worth a pound of cure. It’s not a matter of “if” but “when” the attack happens. The financial costs of such attacks often run much higher than the cost of prevention — not to mention that the financial cost from a cyber event is likely to extend well beyond just headline figures. Additional costs from these tail events can include data restoration, investigation and response, regulatory legal fines, and brand damage. The damage to trust and reputation is also something that you can’t put a number on.

# 9 Challenges & TPx Solutions

## CYBERSECURITY

### Challenge

- Managing high volumes of sensitive data (social security numbers, financial data etc.) and face persistent cyber threats while supporting critical infrastructure
- Frequent targets of ransomware/phishing attacks

  – Usually caused by a staff member’s credentials being compromised through a phishing email, the lack of education and awareness training for staff, and the diminished importance of cybersecurity at all levels.
- SOC is often overburdened thanks to an ever-increasing number of threats
- Many cybersecurity requirements and regulations to adhere to
- May be hard to persuade the Board to invest in cybersecurity BEFORE the attack, not AFTER.
- Endpoints are also a great pain point thanks to a greater need for digitalization due to Covid
- Rising cloud adoption comes with more security concerns
- Rapid and abrupt move to remote and hybrid work results in an expanded attack surface, which creates challenges for managing applications and data outside of traditional networks

### TPx Solution Highlights

1. Conduct a full cyber risk and security assessment across the organization and the network.
2. Consistent, continuous and relevant education and awareness training
3. Deploy key tools to minimize threats

   The baseline has gone from effective backups to endpoint detection (MDR).

   The need for effective threat detection and response is more important than ever as they look to modernize legacy systems and embrace cloud computing.

   The rise of double extortion makes endpoint detection a mandatory component of any security architecture.

## Security Advisory Services

- Cybersecurity Gap Assessment
- Vulnerability & Penetration Scanning
- Network Security Assessment
- Wireless Security Assessment
- FTC Safeguards Rule Preparedness
- Customized Advisory Services

## Cyber Threat Assessment Program (CTAP)

- Get a fast (and free) overview of the status of the customer's network — if there are security issues that need attention, usage or productivity issues
- Obtain power to get more budget for IT

## Managed Endpoints service

- Managed Detection and Response (MDR)
- Managed Inbox Detection and Response (IDR)
- Cybersecurity Awareness Training
- DNS Protection
- Remote Monitoring and Management Agent (RMM)
- Automated Patch Management
- 24/7 Monitoring and Alerting
- Next Generation Anti-virus Agent (NGAV)
- Endpoint AV/AM Deep Scan Assistance & Remediation

## Managed Firewall service

- Managed detection & response
- Threat intelligence
- Sandboxing
- Vulnerability scans
- SD-WAN
- Anti-virus
- Web filtering
- Application control
- Intrusion prevention
- SSL deep packet inspection
- Web application firewall
- Data leak prevention
- Traffic shaping
- Policy scheduling
- Site to site IPsec
- Active directory integration
- VPNs with 2-factor authentication

## Managed Backup service

- Ransomware Detection
- Disaster Recovery Virtualization
- Hybrid On-Premises Backup Device + Cloud Backup Solution
- Device and Cloud Audit Reports
- End-to-end encryption
- Advanced screenshot verification

# CONNECTIVITY

## Challenge

Most financial organizations are distributed. While the advent of cloud and other technologies has made it easier than ever for these entities to operate as a cohesive unit, they also represent a significant challenge for IT teams — and, if managed improperly, can become a large source of operational and financial inefficiency.

Finance is a unique industry with a diverse number of business distribution models. Many such models carry complex, delicate networking needs. Combined with the industry's always-on nature, these factors can turn small disruptions into disasters — and make any change that breaks the complex dependencies of the average institution's network a no-go.

- Facing pressure to provide services virtually: need for scalable, reliable applications, forcing them to move to cloud, fully or at least partially — which causes issues with security and connectivity
- They have security and compliance responsibilities other types of businesses do not
- Traditional MPLS is often expensive and too inflexible
- A need for better control over its network, greater redundancy and more reliability
- A greater need for stability, uptime, and performance
- Rise in remote and hybrid office environment warrants a need for greater connectivity
- Digitalization comes with increased Internet traffic, causing issues with bandwidth capacity
- All banks hate their networks
- Network is not a focal point
- No experts on staff, typically outsourced to core providers who don't know routing
- Antiquated phone systems, still on-premises PBX, not moved to the cloud yet, risk-averse

## TPx Solution Highlights

### Managed SD-WAN

- First and foremost, banks and credit unions often have several branch locations, and SD-WAN is particularly well-suited to simplify how businesses provision and manage networks across several locations.
- Because the banks have increased security and compliance regulations, they find SD-WAN especially appealing, since they can maintain a secure connection via SD-WAN, in which traffic from the branches is backhauled over an encrypted VPN to internal gateways, where TPx can monitor all traffic and enforce security policies.
- With advances like video, mobile banking and digital signage, reliable connectivity will prove key to maintaining a great in-branch experience for bank staff and customers everywhere
- IDC noted that the ability to optimize bandwidth — including traffic from relatively bandwidth-hungry cloud communication solutions — is a leading driver for the move to SD-WAN technology.

> A hybrid WAN utilizing MPLS and SD-WAN technology offers organizations the best of both worlds: a private circuit for the apps that need it and cloud-based WAN for tools that are better suited to public networking options.

- New branches can be added to the WAN with ease, cutting back on one-time implementation costs and ongoing maintenance. Better, the technology's single-pipe networking approach mitigates the impact of disruptions. When networking solutions automatically move to the next-best source in the event of an outage, it's that much easier to rebound. That means no more worrying about a network hiccup taking the bank's walk-in operations out for 15 minutes while IT scrambles to get things back online.

> North Carolina-based Entegra Bank was able to increase connectivity and reduce its bill by 50 percent, while simultaneously maintaining security regulations thanks to a Silver Peak SD-WAN solution.

***Source***

## WAN Solution Highlights

- Provider & transport agnostic
- Network continuity and redundancy
  – Optimal delivery path selection and sub-second failover
  – Leverage the total bandwidth of up to 4 connections OTT, TPx circuit or 4G LTE
- Secure connectivity
  – Dynamic edge-to-edge communication via IPSec VPN connectivity, stateful firewall
- WAN optimization
  – Forward Error Correction (FEC), jitter buffering, link steering/ remediation, and dynamic path selection
- Assured application performance
- Zero-touch deployments
- Potentially significant cost savings: ~25% average expected savings/location moving to SD-WAN (Gartner)
- Easy to scale and reach remote areas

## Managed Networks (Wi-Fi 6)

- SD-WAN/Firewall, Wireless LAN, Network Switches
- Network visibility and control
- Fastest, most reliable network possible
- Security
- 24/7 Monitoring and Alerting
- Troubleshooting
- Configuration Deployment/Management
- Backups/Disaster Recovery
- Firmware Upgrades
- Hardware Assurance
- Licensing/Inventory
- Certified Vendor Expertise

## Access

- Multiple access options
- Superior network redundancy
- Performance quality
- Flexible bandwidth

# COLLABORATION

## Challenge

- Having employees dispersed in many different locations and now with many working from home, they have to address their workers' collaboration needs whilst also maintaining the highest level of security.
- Adapting to a hybrid work environment: ensuring that staff has the assets they need without putting the privacy of data and systems at risk
- Being able to communicate effectively to help assist and serve the public

## TPx Solution Highlights

### UCx with Webex

- Video, phone calling, call center, messaging and meetings all delivered in a single application
- Enterprise-grade security and end-to-end encryption
- Several pre-built integrations to third party applications like Google, Microsoft, Salesforce and more
- Integrated Enterprise VoIP
- instant access to new features and updates as soon as they are available
- Business continuity: Since UCx is hosted on the TPx network, the application will still be accessible in the event of a power outage, fire or other disasters

### UCx Calling for Microsoft Teams

### UCx SmartVoice SIP Trunks

> The success of the initial small trial resulted in a further expansion of Webex Teams to over 1000 employees, spread across multiple regions and to a wider section of the organization. Feedback from their users was exceptionally positive and senior leadership within BBVA quickly made the decision to fully adopt Webex as their collaboration platform of choice."
>
> *Banco Bilbao Vizcaya Argentaria (BBVA)*

***Case Study***

# LACK OF RESOURCES (FUNDING/SKILL SET)

## Challenge

- IT and cybersecurity talent is hard to find and hard to retain
- Funding is always hard to come by
- Having a small IT team that's stretched too thin

## TPx Solution Highlights

- Managed Services Providers can take on things that would be more expensive to do in-house, thus saving you money.
- We can augment your team with experts who are available 24/7, have a narrow specialization (not one person who does it all), who thus have extensive experience doing that specific task for many customers previously.