opengear

WHITE PAPER

Security & Resilience In Financial Networks

In the world of finance, cyberattack is inevitable and frequent. Over the last few years, attacks on the financial sector have gone from small-scale crimes to coordinated efforts to take down entire networks and payment systems. In responding to these ever more sophisticated threats, it's important to add in multiple layers of defense, keeping end-to-end attacks at bay. Going beyond encryption and other security strategies by creating a resilient network helps businesses not only survive cyberattacks but keeps ATMs running, branches open, and apps operating.

This paper takes a look at the security and business risks of network outages and ways you can build a more resilient financial services network.

RECENT FINANCIAL INSTITUTION CYBERATTACKS

Early cyberattacks focused on existing weaknesses in financial network systems that have since been addressed. But malware, phishing, and social engineering attacks grow more sophisticated and prevalent. Hacking software has become easily available to anyone who simply searches for it. And while companies offering security solutions have helped, they have also inadvertently provided information on how to build advanced hacking tools and where to conduct attacks.

Here are some recent examples of successful attacks against financial institutions:

- **February 2, 2019** - UK-based Metro Bank was the first major bank to succumb to a new type of cyberattack that intercepts text messages with two-factor authentication codes used to verify transactions.
- **December 23, 2018** – Evercore, a global investment bank, was breached by hackers who gained access to thousands of sensitive documents.
- **December 18, 2018** - Click2Gov, an online bill-payment portal for local government services, was the victim of a data breach.
- **November 14, 2018** – Two men in Venezuela were found guilty of installing malicious software or hardware on ATMs to force the machines to dispense huge amounts of cash on demand.
- **November 6, 2018** - Hackers gained access to US HSBC customer data including names, addresses, phone numbers, and account information.

These are just a few examples of recent attacks. For a more comprehensive and eye-opening list, visit the Timeline of Cyber Incidents Involving Financial Institutions.

MITIGATING THE CYBERATTACK THREAT

To prevent some of the most egregious threats, today's financial networks must implement SSH key authentication, IPSEC or OpenSSL VPN tunnels, Stateful Firewall, Centralized Logging, Alerting, Remote AAA, and more. And every device in our networks is a potential target, including, and sometimes especially, branch and edge devices. Security and true resilience must be factored in to every aspect of our network infrastructure.

WHAT CAUSES OUTAGES?

Cyberattack | Natural Disaster | Human Error

System outages can result from cyberattacks, natural disasters, construction or vehicle accidents, human error, or any number of environmental conditions.

A wide range of network elements can also cause outages. Cable interconnects, power supplies, switches, dense compute chassis, storage arrays, and even air conditioning are potential sources of problems. And network devices are only increasing in complexity, with software stacks that are frequently updated and susceptible to bugs, exploits, and cyberattacks.

REDUNDANCY IS NOT THE SAME AS RESILIENCE

It's important to understand the difference between resilience and redundancy. While a resilient network may contain some redundancy, a redundant system isn't necessarily sufficiently resilient.

A redundant system duplicates some network elements so that if one path fails, another can be used. For example, you may have duplicate routers or network connections from two different providers. But this doesn't mean that your network is resilient. Resilience considers the full ecosystem, from core to edge, whereas redundancy removes a single point of failure.

And redundancy is expensive. If your company has two separate data connections for network redundancy, you would want to use both connections rather than paying for a connection that is idle 99% of the time. If there is a failure, your network cannot be considered to be resilient when it is now only handling half as much traffic.

REDUCING DOWNTIME IN AN ATM NETWORK

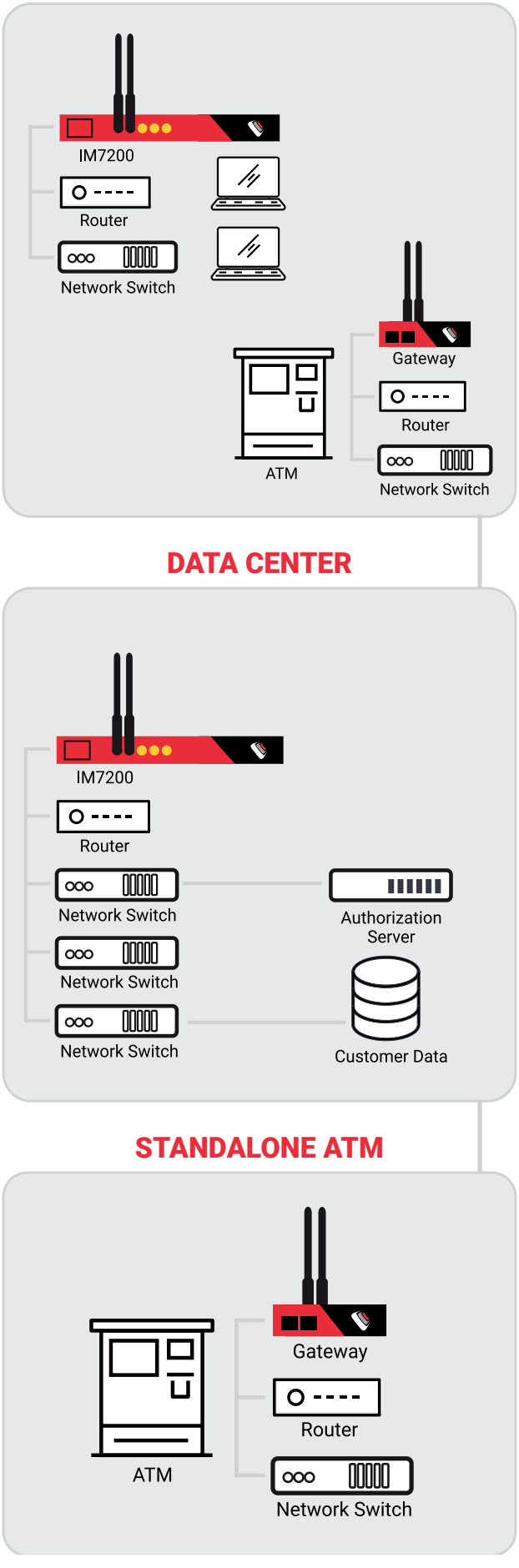
Consider an ATM network with machines in many remote sites. When they go down, it presents not only a loss of revenue and a loss of clients, it's also a security issue. In the past, when an ATM went down, you would have to send an engineer out to open it. It's a security issue and the downtime can be hours or in some cases days.

Banks with ATM networks need something that allows them to get these remote units fixed without having to waste the time driving there and dealing with the security issues of opening the box up. They need something that can give them remote access when the network is up and running and also access when the network is down. And they need something that can allow them to power cycle the equipment within the ATM when the router hangs.

These networks need a solution that is vendor neutral on the equipment it connects to but also vendor neutral on the power equipment that it can manage. An out-of-band management unit can be added to each ATM to reduce downtime to just a few minutes and bring them back up very quickly. It also negates the need for someone to physically go to the site, and most importantly removes the necessity for the secure opening up of the ATM.

KEEPING BRANCHES UP AND RUNNING

Financial networks are moving to SD-WAN solutions to reduce costs and add flexibility across their multiple branches. They need a solution that is as reliable as their data centers, eliminating the risk of a complex router becoming a single point of failure. Ideally, this means uninterrupted Internet connectivity for all branch LANs and equipment over a link that is not part of your production network. Branches need to be able to leverage high-speed networks whenever the primary link is unavailable. One solution is to use *Smart* Out-of-Band (OOB) with Failover to Cellular™ (F2C) technology, which provides enough bandwidth on an alternate path to allow critical functions to keep running until the network event is resolved.



CASE STUDY

Banking Group Adds Out-of-Band Solution

Türkiye Finans, a Turkish Banking group with over a million international customers and more than 250 branches needed to improve detection and resolution of its IT systems. This growing business also needed help to streamline and accelerate the setup of new locations. It needed an Out-of-Band management solution for its dispersed branch sites.

The main considerations were:

- Ensure secure communications with strong data encryption
- Provision, maintain and repair systems with built-in Out-of-Band access and control
- Serve both data center and branch sites with a scalable product offering
- Provide competitive pricing versus performance aspect with non-restrictive upgrade policy

Wanting to specifically work with a proven technology supplier, Türkiye Finans chose Opengear. The bank specified an array of remote site products, which have been rolled out to 145 sites, to enable secure remote monitoring, access, and control of its distributed install.

> ***"Opengear saves us time and allows us to quickly understand and resolve a wide range of problems and ultimately increase customer satisfaction."***
>
> *~ Erdal Ek, Senior Network Specialist, Türkiye Finans*

This solution has given network admins an easy way to upload managed infrastructure configuration and operating system images from the device's internal flash drive for remote bare metal provisioning of critical systems. Also, it has improved the IT department's ability to manage and configure remote devices during installation or if a challenge arises.

The bank has upgraded each branch and integrated a secure serial console server and PSTN dial-in gateway with stateful firewall at each location to ensure the security compliance necessary for financial transactions.

MORE DATA, GREATER RISK

More than any other industry, financial services must provide consumers ways to conduct transactions through mobile devices. By 2025, Millennials will generate 46 percent of all U.S. income. 38 percent use apps and mobile tools to make bill payments. 27 percent of Millennials are completely reliant on a mobile banking app for regular banking activities.[1]

For financial firms, the ability to offer such online services represents a huge competitive advantage.

To handle growing data needs, financial institutions are moving to cloud environments. Unfortunately, this means customer data is spread across an ever-larger potential cyberattack surface. Financial services must focus on protecting the private data of consumers. One solution is to add in secure alternate access.

FINANCIAL SERVICES NEED RESILIENT NETWORKS

Outages are bad news for financial institutions, but they are inevitable because of human error, cyberattack, and the ever-increasing complexity of network devices, modern software stacks, and hardware devices. To keep consumers happy and the institution's reputation intact, financial services must be prepared for outages. *Smart* OOB™ with Failover to Cellular can keep services running even when part of the network is down.

1 - https://www.salesforce.com/form/marketingcloud/what-millennials-expect-from-their-banks.jsp