

CELENT



FORCHT BANK: CYBERSECURITY EXCELLENCE THROUGH STRATEGIC OUTSOURCING

**WINNER OF CELENT MODEL RISK MANAGER 2022 AWARD FOR
LEGACY AND ECOSYSTEM TRANSFORMATION**

March 15, 2022

Neil Katkov, PhD

This is an authorized reprint of a Celent report profiling a Model Risk Manager Award winning technology initiative and was not sponsored by Forcht Bank or Fiserv in any way. Reprint granted to Fiserv. For more information, please contact Celent (www.celent.com) or info@celent.com.

CASE STUDY AT A GLANCE

Forcht Bank, a community bank operating in Kentucky and Ohio, aimed to strengthen cybersecurity by leveraging managed services on the strategic principle that, through outsourcing, small banks can implement services, security, and infrastructure comparable to larger institutions.

Forcht Bank's managed cybersecurity services include an outsourced Security Operations Center (SOC) team as well as a range of cybersecurity tools. In addition to greatly reducing the bank's on-premise technology footprint, outsourcing cybersecurity removes the burden of maintaining an in-house SOC team and managing multiple vendor relationships for the tools.

Forcht Bank's cybersecurity technology is deployed on Microsoft Azure on a hybrid cloud model and managed by Fiserv. Managed SOC services are provided by BlueVoyant.

Key benefits realized by the initiative include significant cost savings, reduction of the IT staff to a core team focused on governance and strategy, access to advanced technology and industry best practice through managed service providers, and a more secure environment for the bank and its customers.

FINANCIAL INSTITUTION	Forcht Bank
INITIATIVE	Cybersecurity Excellence through Strategic Outsourcing
SYNOPSIS	Forcht Bank leveraged cloud-based managed services deployed on a hybrid cloud model to achieve a cybersecurity posture comparable to large institutions.
TIMELINES	<ul style="list-style-type: none"> • Project implementation: Q1 2020 – Q4 2021
KEY BENEFITS	<ul style="list-style-type: none"> • Vendor technology savings • Reduction of inhouse IT staffing • Access to advanced technology and industry best practice
KEY VENDORS	Fiserv, Microsoft, BlueVoyant

CELENT PERSPECTIVE

Cybersecurity is a technologically and operationally complex domain, requiring myriad tools, highly trained response teams, and increasingly advanced analytic and data science capabilities. It was a clear win for Forcht Bank to outsource its technology infrastructure to experienced providers, freeing themselves to focus on the strategic planning and governance aspects of cybersecurity.

In this initiative, Forcht Bank leveraged managed services to improve their cybersecurity posture beyond what a smaller institution can typically achieve.

Cyber threats against banks and other financial institutions continue to grow in sophistication and intensity, a trend fueled by the expansion of cloud-based and digital financial services. Community banks are not spared from the increasing risk and may lack capacity to effectively deploy the advanced tools and techniques needed to ensure a secure environment.

The bank's vision for its new infrastructure was ambitious for an institution of any size. Carl Clements, Executive Vice President at Forcht Bank and the sponsor of the project, aimed for a holistic approach to cybersecurity that aggregated data from as many tools and services as possible into a "single pane of glass" dashboard to generate actionable alerts.

Clements also knew it was vital to leverage emerging technologies, such as machine learning, and a zero trust security model in order to ensure the integrity of the banking environment in the face of incessant cyber attacks.

The bank chose an existing partner, Fiserv, to manage the technology, leveraging Fiserv's expertise in Microsoft's suite of cybersecurity tools hosted on Azure. The relationship provides Forcht Bank with access to world-class technology and analytics and a sustainable approach to keeping up with the rapidly evolving cybersecurity space.

Forcht Bank's decision to outsource its cybersecurity operations was part of a larger transformation project to migrate its technology to a hybrid cloud infrastructure. Managed services have produced substantial savings on both vended technology and internal IT costs. It has enabled the bank to reduce its entire IT staffing model to five people, who now focus on governance and vision. As Clements puts it, Forcht Bank's managed services partners "can do the heavy lifting and we can do strategy."

DETAILED DESCRIPTION

Forcht Bank is a community bank operating in Kentucky and Ohio. Founded in 1985, the bank acquired 10 other community banks over the next two decades. The bank's mission statement focuses on respect for the customer, competitive rates, and service to the community. Forcht Bank was named Best Bank in Kentucky by Forbes in 2021 and, according to the bank, its improved infrastructure was a key factor in achieving this recognition.

Forcht Bank sought to ensure a robust and sustainable cybersecurity posture comparable to larger financial institutions. To achieve this goal, the bank decided to rely on a managed services infrastructure integrating multiple cybersecurity tools and services into a cohesive environment, with governance provided by the bank.

Table 1: Forcht Bank Snapshot

	Forcht Bank
YEAR FOUNDED	1985
TOTAL ASSETS	US\$1 billion
GEOGRAPHICAL PRESENCE	Kentucky and Cincinnati, Ohio
EMPLOYEES	Approximately 300
RELEVANT TECHNOLOGIES AND VENDORS	Fiserv, Microsoft, BlueVoyant

Source: Forcht Bank

Opportunity

Forcht Bank's cybersecurity initiative was part of a transformation program to migrate the bank's IT infrastructure and security tools to a hybrid cloud environment. The bank saw outsourcing to strategic partners as a way to access world-class technology while at the same time reducing costs.

Specific requirements for the initiative included:

- The ability to manage, monitor, and restrict the bank's new cloud-based applications due to their potential vulnerability to attack
- Implementing a zero trust model and real time access analysis to identify and block unusual log-in attempts
- A unified "single pane of glass" console for aggregating security data, reports, and alerts from multiple tools and services, allowing Forcht Bank to operate with minimal IT security staffing
- A multi-layered email defense strategy including anti-phishing, DMARC authentication to protect against email compromise, and other techniques
- Vulnerability remediation, firewall, and data protection services
- Support for business continuity and resiliency

Solution

The bank chose Fiserv to manage the technology, which was deployed on a Microsoft hybrid cloud environment. The platform includes Microsoft security tools hosted on Azure, including the Microsoft Defender security stack and Azure Sentinel, as well as Splunk and various other tools. Managed SOC services are provided by BlueVoyant on a 24/7 basis.

The technology stack covers a full range of cybersecurity functions, including:

- Multifactor authentication (MFA) with a focus on biometric authentication
- A privileged access management (PAM) solution with MFA, to manage access to servers and critical resources
- Email defense, anti-phishing, and anti-spoofing
- Anti-malware security
- Intrusion prevention
- Patching and security update management
- Data backup and high-availability infrastructure, including redundant SD-WAN connections

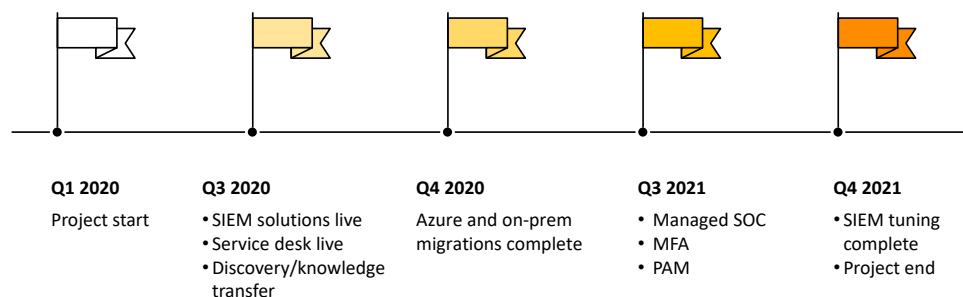
Implementation and Timeline

Forcht Bank's cybersecurity transformation involved many moving parts and overlapping implementation activities. The project launch coincided with the emergence of the COVID-19 pandemic, requiring the bank and its partners to develop remote working methods. Nevertheless, the initiative proceeded at a smooth pace, starting in January of 2020 and ending in October 2021.

Some of the key milestones of the initiative included:

- Project start: Q1 2020
- Azure migration: Q2 – Q4 2020
- Discovery and knowledge transfer completed: Q2 2020
- Azure and Splunk SIEM solutions: Q3 2020
(Splunk tuning completed Q1 2021; Azure Sentinel tuning completed Q3 2021)
- Physical network: Q4 2020 – Q3 2021
- SD-WAN: Q2 – Q3 2021
- Multifactor authentication: Q3 2021
- Privileged access management: Q3 – Q4 2021
- Managed SOC go-live: Q3 2021

Figure 1: Forcht Bank Cybersecurity Managed Services Implementation Timeline



Source: Forcht Bank

Results

The move to managed services strengthened the bank's cybersecurity posture, substantially reduced IT costs, and allowed Forcht Bank to reduce the size of its IT team to a core group focused on IT governance and strategy.

The bank has experienced a progressive decrease in pending critical vulnerabilities, patches, and security updates. As a result, Forcht Bank rose from the 50th percentile

of peer banks to the 95th percentile for vulnerability management, according to an assessment by Fiserv.

Forcht Bank now has greater visibility into their current cybersecurity status through a unified console for managed detection and response (MDR), vulnerability, and managed SIEM.

The bank is also able to provide a safer and more secure environment for its customers. This improves trust, an increasingly important factor as digital financial services potentially expose the bank and its customers to new threats.

Fundamentally, managed services provide Forcht Bank with ongoing, sustainable access to world-class technology. As Carl Clements puts it, through its managed services partners, the bank is “able to leverage the relationships that they have and their expertise in this area, and they help us improve our security posture through regular strategy sessions. So it’s been a win for the bank all the way around.”

Lessons Learned

Both the executive management and users supported Forcht Bank’s transformation program. Looking back, though, the bank feels that with a project of this size and scope, they might have slowed the implementation pace to reduce the stress on the bank’s teams and users who had to adapt to rapid change.

Considering the demand on resources and time that a migration of this size entails—and the fact that team members also had full-time regular responsibilities—the bank also learned the importance of reallocating employee duties at the beginning to ensure the team has sufficient time and resources to complete the project.

Finally, Clements stresses the need to be open to dialogue and feedback as a means to overcome disagreements. As he put it, “Problems will arise. Don’t waste time blaming. Solve the problem instead.”

The Way Forward

Building on the positive outcomes of its strategy to move cybersecurity to a managed services footing, Forcht Bank plans to continue to work closely with its technology partners to identify opportunities for enhancing cybersecurity capabilities and effectiveness through continual process improvement, new product offerings and services, and industry best practices.

LEVERAGING CELENT'S EXPERTISE

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

Support for Financial Institutions

Typical projects we support include:

Vendor short listing and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes and requirements. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

Support for Vendors

We provide services that help you refine your product and service offerings.

Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials—including your website and any collateral.

RELATED CELENT RESEARCH

[Remaking Risk: A Taxonomy of Regtech](#)

October 2021

[Technology Trends Previsory: Risk, 2022 Edition](#)

October 2021

[Transforming Adverse Media Screening: A New Paradigm Powered by AI](#)

June 2021

[IT and Operational Spending in AML-KYC: 2021 Edition](#)

December 2021

[IT and Operational Spending on Fraud: 2021 Edition](#)

February 2021

[Innovation In Risk: A Snapshot Through the Lens of Model Risk Manager 2021](#)

April 2021

[Reimagining Watchlist Screening: Improving Efficiency and Effectiveness with Modern Technologies](#)

July 2021

[HSBC: Insurance-focused Transaction Monitoring Solution Powered by Machine Learning and Cloud](#)

March 2021

[Goldman Sachs: Machine Learning-Powered Watchlist Screening Tool](#)

March 2021

[Fino Payments Bank: Remote Implementation of Enterprise-Wide Fraud Management During the Pandemic](#)

March 2021

[Standard Bank: KYC On The Go – A Component of Remote Customer Onboarding](#)

March 2021

[Swedbank: Modernizing Card Fraud Management and Improving Customer Experience](#)

March 2021

[Know Your Customer Systems: 2020 xCelent Awards, Powered by VendorMatch](#)

June 2020

COPYRIGHT NOTICE

Copyright 2022 Celent, a division of Oliver Wyman, Inc., which is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. All rights reserved. This report may not be reproduced, copied or redistributed, in whole or in part, in any form or by any means, without the written permission of Celent, a division of Oliver Wyman ("Celent") and Celent accepts no liability whatsoever for the actions of third parties in this respect. Celent and any third party content providers whose content is included in this report are the sole copyright owners of the content in this report. Any third party content in this report has been included by Celent with the permission of the relevant content owner. Any use of this report by any third party is strictly prohibited without a license expressly granted by Celent. Any use of third party content included in this report is strictly prohibited without the express permission of the relevant content owner. This report is not intended for general circulation, nor is it to be used, reproduced, copied, quoted or distributed by third parties for any purpose other than those that may be set forth herein without the prior written permission of Celent. Neither all nor any part of the contents of this report, or any opinions expressed herein, shall be disseminated to the public through advertising media, public relations, news media, sales media, mail, direct transmittal, or any other public means of communications, without the prior written consent of Celent. Any violation of Celent's rights in this report will be enforced to the fullest extent of the law, including the pursuit of monetary damages and injunctive relief in the event of any breach of the foregoing restrictions.

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification.

Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

There are no third party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report.

No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

For more information please contact info@celent.com or:

Neil Katkov

nkatkov@celent.com

Americas

USA

99 High Street, 32nd Floor
Boston, MA 02110-2320

[+1.617.262.3120](tel:+1.617.262.3120)

USA

1166 Avenue of the Americas
New York, NY 10036

[+1.212.345.3960](tel:+1.212.345.3960)

USA

Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

[+1.415.743.7960](tel:+1.415.743.7960)

Brazil

Av. Dr. Chucri Zaidan, 920
Market Place Tower I - 4^o Andar
Sao Paulo SP 04583-905

[+55 11 5501 1100](tel:+55.11.5501.1100)

EMEA

Switzerland

Tessinerplatz 5
Zurich 8027

[+41.44.5533.333](tel:+41.44.5533.333)

France

1 Rue Euler
Paris 75008

[+33 1 45 02 30 00](tel:+33.1.45.02.30.00)

Italy

Galleria San Babila 4B
Milan 20122

[+39.02.305.771](tel:+39.02.305.771)

United Kingdom

55 Baker Street
London W1U 8EW

[+44.20.7333.8333](tel:+44.20.7333.8333)

Asia-Pacific

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

[+81.3.3500.3023](tel:+81.3.3500.3023)

Hong Kong

Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

[+852 2301 7500](tel:+852.2301.7500)