BISHOP FOX®

The Gold Standard in Security Consulting

Table of Contents

Bishop Fox was founded in 2005 on the principle that all we do is advise our clients, so they make the best possible security decisions.

Security Is Hard, But Not Impossible

We live in exciting times. The rate of technological advancement has changed the world in ways that were previously unimaginable. Cars are driving themselves, drones are being used to deliver medicine during disasters, and colorful smartphone apps are processing sensitive data for global financial institutions.

We've become numb to the sheer volume of data breaches and losses from financially motivated cybercrime. Even in the most mature organizations with well understood network infrastructures, it's becoming near impossible to keep intruders from accessing the tsunami of data traversing our networks.

The harsh truth is that the majority of targeted attacks, privacy disasters, and data breaches are caused by negligence and innocuous mistakes: poor password policies, social engineering (phishing), misconfiguration in a software system or cloud service, and poor patch management (insecure application).

One simple mistake can have debilitating consequences but, as we look to the future, it's reassuring that cybersecurity is attracting the highest levels of attention. Security practitioners are no longer taking a defeatist attitude, or become overwhelmed by the magnitude of the problem. I'm encouraged to see security leaders taking a proactive approach to risk management, embracing tools and human expertise to address problems and keep attackers at bay.

Let's not sugarcoat the truth: security is very hard. But it doesn't have to be impossible.

Vincent Liu, Founder and Managing Partner

Three Good Reasons To Work With Us

Objectivity - Experience - Results

1 - Objectivity

Our mission is to deliver transparent, sustainable, and value-based security advice to help our clients make the best possible security decisions.

We favor an independent and vendor-agnostic consulting model that ensures our objectivity—our obligation is to our clients and ***only*** our clients—we have no proprietary products and no revenue-sharing arrangements with other organizations.

2 - Experience

We have gained significant expertise since our founding in 2005. Our exposure to Fortune 100 organizations and to innovative technology start-ups has helped us understand the security challenges that come with exponential growth and innovation.

Experience has also taught us that specialized expertise matters. Our consultants combine more than 500 years of wide-ranging professional experience. Our senior consultants collaborate closely with all members of our clients' team.

3 - Results

In our world, success is determined by the ability of our clients to implement long-term and sustainable security programs at the best value.

Bishop Fox has earned its distinguished reputation through a decade of solid and untarnished security practices. Our high client-retention rate and consistent recognition by peers and national publications are a tribute to our solid foundation.

Bishop Fox Clients

We provide security consulting services to the Fortune 1000 and high-tech startups.
We are trusted by peers and industry leaders.

5 of the Top 10
Global Media Organizations

10 of the Top 20
Global Retailers

26 of Fortune 100
Organizations

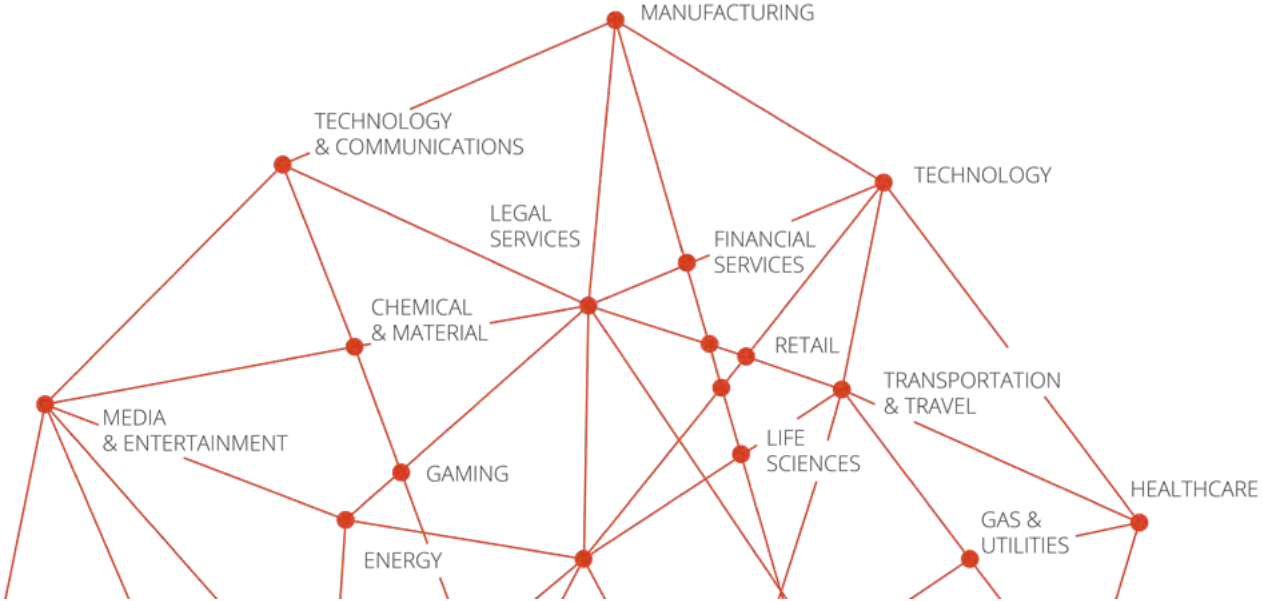
6 of the Top 10
Manufacturing Organizations

8 of the Top 10
Global Technology Organizations

Our customers are always happy to share their experience and knowledge.
Ask us for references.


Trusted by 26
of the Fortune 100

Expertise in Multiple Industries



Our Services

We develop tailored programs to secure companies against present and future threats.

Application Security

- Application Penetration Testing
- Hybrid Application Assessment
- Mobile Application Assessment
- Source Code Review

Network Security

- Network Penetration Testing
- PCI ASV Quarterly Scanning
- Wireless Penetration

Infrastructure Security

- Physical Penetration Testing
- Social Engineering
- Telephony Penetration Testing

Architecture Security

- Architecture Security Assessment
- Threat Modeling

Cloud Security

- Design Review
- Deployment Review

Integrated Services

- External Penetration Testing
- Internal Penetration Testing
- Product Security Review
- Third-party Assessment
- Risk Assessment
- Red Teaming

Technical Controls

- Technical Control Review
- CIS Critical Security Controls
- Firewall Review
- Host-based Configuration Review

Managed Services

- Continuous Penetration Testing

We Bring Technical Depth To Our Clients

Meet our leadership team.

Vincent Liu, Founder & Managing Partner

With nearly two decades of experience, Vincent Liu is an expert in security strategy, red teaming, and product security; he oversees firm strategy and client relationships. He is regularly cited and interviewed by media such as Al Jazeera, The Information, and NPR while also writing as a contributing columnist for Dark Reading. He has co-authored books including Hacking Exposed Wireless and Hacking Exposed Web Applications. Vincent sits on several advisory boards in addition to serving as returning faculty at the Practising Law Institute.

Francis Brown, Founder & Partner

Francis focuses on running service delivery and heading the thought leadership program. Francis has presented his research at leading conferences such as Black Hat USA, DEF CON, InfoSec World, ToorCon, RSA, and HackCon. His research has been featured in USA Today, Forbes, InformationWeek, and Dark Reading. Francis is the creator of the Tastic RFID Thief (which has appeared on “Mr. Robot”), the Danger Drone, and the SearchDiggity Project.

Christie Terrill, Partner

Christie has provided security advisory services for over a decade. Her focuses are engagement oversight, thought leadership, and relationship management. Christie is a contributor to Forbes.

Justin Hays, Partner

Justin focuses on all aspects of security testing and design in addition to firm-wide research endeavors. Justin actively conducts mobile device and web application security research.

Carl Livitt, Partner

Carl has decades of experience in mobile and application security, hardware, reverse engineering, and global-scale penetration testing.

Rob Ragan, Partner

Rob provides security solutions and strategy to Bishop Fox clients. His other focuses include red teaming and threat modeling. He also manages the San Francisco consulting team.

Andrew Wilson, Partner

Andrew is responsible for managing our consulting practice. He is a Microsoft Developer MVP and has presented at DEF CON, BSides, ToorCon, and AppSec. He is the founder of the security conference CactusCon.

Gwenyth Castro, Chief Revenue Officer

Gwenyth oversees the implementation of both long and short-term strategic plans. Additionally, Gwenyth mitigates risks for the company as whole.

We Are Passionate

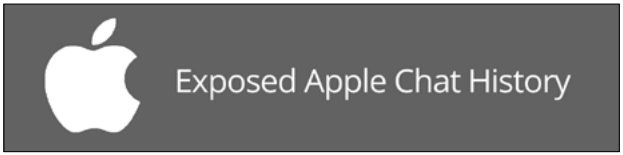
Our team researches and continuously learns about what is happening in the industry.

As one of a handful of professional services firms that regularly conducts cutting-edge research, we're able to provide our clients with true insight into emerging risks.

Some of our findings:

Critical DNS Flaw Exposes Windows Computers

A critical vulnerability affecting millions of Windows users allows attackers to insert malicious payloads, execute arbitrary code with the permission of an application like a web browser or any software that uses DNS, and take complete control over a target computer or server.

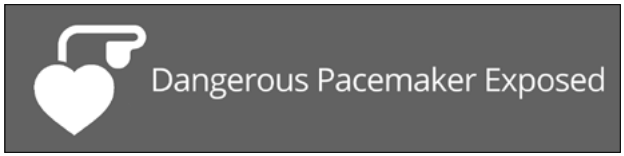


Apple Bug Exposed Chat History With a Single Click

A major vulnerability in Apple's iMessage could be exploited by hackers to pull a target's message history through a bogus link. Once clicked, the link pulled data from within the iMessage application and exported it to an outside source.

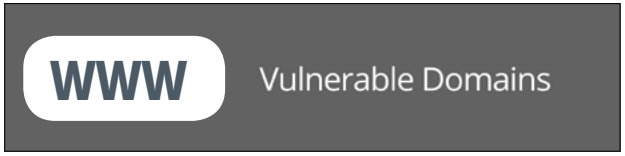
Drones Emerge as New Dimension in Cyberwar

Past proof of concepts have already demonstrated the threat is real. Bishop Fox puts the first generation of drone defense solutions to the test by creating a penetration testing drone capable of launching fly-by exploits and security assessments. The project includes a comprehensive testing of existing anti-drone systems.



Dangerous Pacemaker Vulnerabilities Confirmed

Muddy Waters and MedSec contracted Bishop Fox to provide an expert opinion on implantable cardiac devices made by St Jude. Our experts found that the statements made by Muddy Waters and MedSec are accurate and that St Jude products "do not meet the security requirements of a system responsible for safeguarding life-sustaining equipment implanted in patients."



98% of the Top Million Domains Potentially Vulnerable to Email Spoofing

Bishop Fox researchers analyzed the Alexa top million Internet domains and found that 98% – nearly the entire Internet – are potentially vulnerable to email spoofing.

Security Risks Doom LinkedIn 'Intro' Service

LinkedIn discontinued its 'Intro' software offering after Bishop Fox researchers warn risks of man-in-the middle attacks.

We Contribute to the Community

Our free security tools are developed by our Bishop Fox team and are available to the public. We are happy to give back to the community that has given us so much.

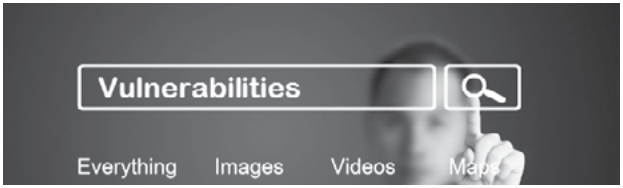
Sample of our tools:

DANGER DRONE is a practical guide to Drone hacking for penetration testers. Helping equip security professionals with the tools to test the effectiveness of their drone defenses and eliminate exposed attack vectors.

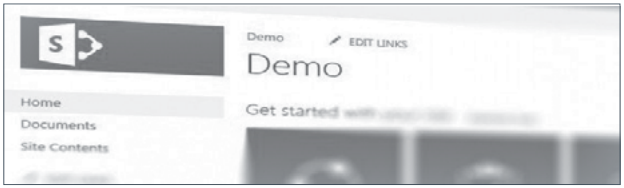
FIRECAT is a penetration testing tool that allows you to punch reverse TCP tunnels out of a compromised network.

RFID HACKING investigates the latest attack tools and techniques available for stealing and using RFID proximity badge information to gain unauthorized access to buildings and other secure areas. Our research has been featured in “Mr. Robot”.

CYBERSECURITY STYLE GUIDE Our editorial team has released a cybersecurity style guide which is intended to be a resource for all different types of audiences.



GOOGLE HACKING DIGGITY PROJECT is a research and development initiative dedicated to investigating Google Hacking, i.e. the latest techniques that leverage search engines, such as Google, Bing, and Shodan, to quickly identify vulnerable systems and sensitive data in corporate networks.



SHAREPOINT HACKING DIGGITY PROJECT is a research and development initiative dedicated to tools and techniques in hacking Microsoft SharePoint technologies. Assessment strategies are designed to help administrators and security professionals identify insecure configurations and exposures introduced by vulnerable SharePoint deployments.

SPOOFCHECK is a tool designed to help you identify if your site is vulnerable to email spoofing. If you are found to be vulnerable, we recommend ways you can make your domain immune to this attack.

MD5 AND MD4 COLLISION GENERATORS
Create MD4 and MD5 hash collisions using groundbreaking new code that improves upon the techniques originally developed by Xiaoyun Wang.


4.0

Our Certifications

We have earned many certifications including the Six Sigma Greenbelt and the DFSS certifications.

We Are Recognized Security Experts

We are regularly cited, quoted, and interviewed in both mainstream and industry media.

Forbes

Why You Need To Worry About Wire Fraud
Managing Security Associate Rob Ragan discusses situations where BEC could affect organizations.

THE WALL STREET JOURNAL.

An Unexpected Security Problem In The Cloud
Partner Vincent Liu discusses common configuration errors that can leave corporate data vulnerable.

FORTUNE

Sarahah Has Been Downloading All The Data In Your Address Book
Discovery made by Bishop Fox Senior Analyst Zach Julian.

CSO

465,000 Pacemakers Vulnerable To Hacking Need
Real security concern following a research done by Bishop Fox.

WIRED

Watch A Test Of Anti-Drone Weapons, From Shotguns To Superdrones
Features Bishop Fox Partner Francis Brown

TechCrunch

Can The Security Community Grow Up?
Features Partner Francis Brown and Security Analyst David Latimer's "Game of Drones" presentation.

International Business Times

Sarahah Collects Contact For Feature That Doesn't Exist

"The discovery was made by Bishop Fox Senior Analyst Zach Julian."

c|net

A Hacker's Next Target Is Just A Web Search Away

"Diggity creator Fran Brown said his tools help people who are defending websites and computer networks... to find out when their systems are leaking sensitive information."

REUTERS

Hired Experts Back Claims St.Jude Heart Devices Can Be Hacked

"Muddy Waters said that outside experts it hired validated its claims that cardiac implants are vulnerable."

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Hackers Can Execute Code On Windows Via DNS Responses

"Critical Windows DNS client vulnerability could allow attackers to target victim's computers."

The Intercept_

Apple Bug Exposed Chat History With One Single Click

"The team that discovered the bug at security consultancy Bishop Fox posted a technical write-up and code demonstrating how to exploit the flaw."

USA TODAY

Will LinkedIn's New 'Intro' Feature Attract Hackers?

"From a security and privacy standpoint, this introduces fresh opportunities for bad guys, says Carl Livitt, Senior Security Researcher at Bishop Fox."

We Are Global

Consultants in 10 locations across the globe

Success Stories

Our stories feature real-world security scenarios.
You'll discover varied approaches adopted by your peers in partnering with Bishop Fox.

EVALUATING SECURITY OF AN INDUSTRIAL IOT PLATFORM | IOTIUM SOLUTION FOR IIOT

SECURING BOOST.BEAST | A NON-TRADITIONAL SOURCE CODE REVIEW

AUGUST | SECURITY ON LOCK

COINBASE AND HACKERONE | MANAGING SECURITY THROUGH COLLABORATION

ZEPHYR HEALTH | BUILDING A HEALTHY SECURITY PROGRAM

CHANGE HEALTHCARE | SECURING A COMPETITIVE ADVANTAGE

EVALUATING SECURITY OF AN INDUSTRIAL IOT PLATFORM

Customer	IoTium Inc
Website	www.iotium.io
Organization	Software
Services Provided	Application Security and Penetration Testing

Summary

- IoTium engaged Bishop Fox to assess the security of its platform, including the web-based IoTium Orchestrator and the hardware-based IoTium iNode.
- Bishop Fox conducted a thorough review of both platform components and delivered a detailed report of findings and recommendations.
- IoTium's engagement with Bishop Fox represents their commitment to the security of its platform and providing peace of mind to their customers.
- IIoT represents a ripe new attack vector; IoTium is setting a precedent by priotirizing security.

Scan the Qr code to watch the video

About IoTium

IoTium is the industry's first commerically deployed, secure infrastructure company for Industrial IoT (IIoT). IoTium bridges the legacy world with the new cloud-enabled world. In the past, when a piece of equipment was malfunctioning, a technician would have to be physically on site to plug into the equipment to diagnose and assess any issues. The IoTium platform plugs into these already existing ports and connects the equipment to the cloud. This allows the same technician to monitor equipment from a remote location.

The Solution

As the first commercially deployed infrastructure company for the Industrial IoT, the security impact is clear. A proactive approach to security and providing peace of mind to customers is IoTium's number one priority. The company needed a third-party security verification to ensure that its platform was secure. IoTium decided to hire a third-party firm to assess the security of the hardware, software, and cloud component of the IoTium offering.

The Result

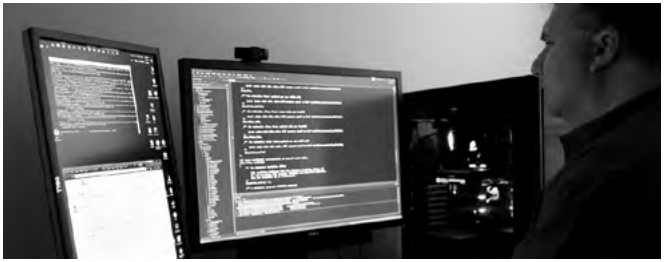
Bishop Fox started with a thorough black-box test of the IoTium offering and delivered a detailed security report to the IoTium product and engineering teams. Working with the IoTium team, Bishop Fox enhanced IoTium's security posture and validate the steps made to correct all identified issues.

> *"Bishop Fox delivered on every one of the goals we outlined for them. They were a pleasure to work with and I would absolutely recommend them to anyone."*

SRI RAJAGOPAL, CHIEF TECHNOLOGY OFFICER AT IOTIUM

SECURING BOOST.BEAST

A NON-TRADITIONAL SOURCE CODE REVIEW



Customer	Vinnie Falco, Founder and President of C++ Alliance; Creator of Beast
Website	https://github.com/boostorg/beast
Organization	C++ header-only library
Services Provided	Application and source code security assessment

Summary

- Beast engaged Bishop Fox to assess the security of their C++ code library.
- Bishop Fox's hybrid application assessment methodology was used alongside targeted source code review and fuzz testing.
- Multiple "high-risk" denial-of-service vulnerabilities were identified and fixed prior to code release.
- Beast's engagement with Bishop Fox reflects the open-source project's commitment to security and transparency.
- Detailed report of the findings is available here: goo.gl/ZFWW4e.

Scan the Qr code
to access the report

The Challenge

Since tens of thousands of users across the Internet rely on the Beast library as the foundation of their code, security and peer review is crucial and mandatory to identify and remove dangerous security vulnerabilities. Vinnie Falco, the creator of Beast, reached out to Bishop Fox to assess the security of the Boost C++ Beast HTTP/S networking library.

The Result

The Bishop Fox assessment team discovered multiple "high-risk" denial-of-service vulnerabilities that could be exploited by malicious hackers to prevent authorized users from accessing the resource.

The team demonstrated three denial-of-service attacks against Beast by sending malformed WebSocket frames containing a compressed payload. The issues were identified by fuzzing the WebSocket server code responsible for uncompressing client messages.

The Solution

Bishop Fox produced a detailed report of the findings, outlining where security vulnerabilities could potentially affect developers when using Beast code as foundation. The crash in WebSocket frames vulnerability was fixed in the first official release of Beast in Boost thanks to the Bishop Fox discoveries. The other vulnerability was found to only affect WebSocket clients in very limited circumstances.

> *"Bishop Fox's reputation in the industry is exceptional. This project was uniquely challenging as it did not fit the typical profile and scope of an application pen-test. Despite the challenges, Bishop Fox was extremely professional and produced great results."*

VINNIE FALCO, FOUNDER AND PRESIDENT
OF C++ ALLIANCE; CREATOR OF BOOST.BEAST

SECURITY ON LOCK

HOME SECURITY MEETS CYBERSECURITY

Customer	August
Website	august.com
Industry	Internet of Things (IoT)
Services Provided	Infrastructure Security on digital and physical devices, Architecture Security, Integrated Services

Summary

- August Home sought a firm that could assess all aspects of their product — hardware, firmware, and software. Their search led them to Bishop Fox.
- The Bishop Fox team reviewed the encryption design and authentication model of the lock as the August team was designing it.
- August Home's commitment to the security and well-being of its customers led to a well-designed and industry-leading product — a product that we at Bishop Fox use in our own offices.

Scan the Qr code to access the case study

The Challenge

August Home had to solve the challenges introduced by hosting their product's functionality in the digital rather than physical realm — they needed to secure homes without introducing backdoors to the back door. Bishop Fox brought their top mobile experts and leading product security researchers in to assess the project.

The Result

August Home put the security of their product and their customer's peace of mind at the forefront of their design. As a result of their partnership with Bishop Fox, their Smart Lock went to market with two-factor authentication, Bluetooth Low Energy (BLE) technology encryption, and an update feature that allows August Home to seamlessly release security advancements to users.

The Solution

As the August team designed the encryption and authentication model for the lock itself, Bishop Fox's team reviewed the design as they were doing it. Working together during the encryption design allowed August Home to build solid IoT security in to all aspects of their Smart Lock before deployment.

> *"Bishop Fox is a group of security professionals who are experts in their field. They brought a number of different disciplines to the project, people who understood all aspects of what we were working with."*

CHRIS DOW, VICE PRESIDENT OF SOFTWARE,
AUGUST HOME

MANAGING SECURITY THROUGH COLLABORATION

coinbase

10M+ USERS

$50B+ TRADED

Customer	Coinbase Inc.
Website	coinbase.com
Industry	Financial Services
Services Provided	Network and Architecture Security Integrated Services

Summary

- Coinbase is the world's leading platform for buying and selling Bitcoin. The Bitcoin network touches thousands of computers and millions of participants globally.
- Operating a bug bounty program was the natural next step in securing Coinbase service, but managing a new initiative within their already busy security program would take away time from progress on other projects.
- By combining the HackerOne platform with Bishop Fox security consultants, Coinbase successfully implemented an effective bug bounty program to improve site security.

Scan the Qr code to access the case study

The Challenge

Coinbase adopted the HackerOne platform to access the world's top security researchers, manage vulnerability reports, and pay bounties; they engaged Bishop Fox to help oversee and validate the inbound report queue.

The Result

Audits are static. A bug bounty program means eyes are always on the product, seeking vulnerabilities. The combination of Bishop Fox expertise and the HackerOne platform simplified the act of receiving, confirming, and responding to reported vulnerabilities, and also provided a practical solution for Coinbase and its vendors to keep their users safe.

The Solution

HackerOne's practical and intuitive service combined with Bishop Fox's security smarts eliminated the stress of implementing a bug bounty program. Coinbase realized that all companies can benefit from managing a bug bounty program – no matter the size or industry. It ensures a certain level of security is maintained.

> *"With Bishop Fox managing our queue, our engineers have more time to focus on our core product. Hiring and optimizing time is a challenge in this industry. Bishop Fox helps improve the efficiency of HackerOne's already excellent service and focus of our team."*

COINBASE SECURITY ENGINEER

BUILDING A HEALTHY SECURITY PROGRAM

Customer	Zephyr Health, Inc.
Website	zephyrhealth.com
Industry	Healthcare Software Vendor
Services Provided	Application, Architecture, and Infrastructure Security

Summary

- When Zephyr Health needed help keeping sensitive data secure, they turned to Bishop Fox. Their customers were asking them what they were doing for security.
- We realized they needed to become compliant with a new security standard in order to better develop and maintain their customers' trust.
- We helped Zephyr Health passed their SOC2 certification in six months from start-to-finish.
- Customers have reported they feel confident Zephyr Health takes their role as a data custodian seriously.

Scan the Qr code to access the case study

The Challenge

As an analytics startup serving the healthcare industry, Zephyr Health needed a solid data security plan that they could demonstrate to their clients. They wanted to focus on company security in a more methodical way. They needed the ability to honestly and accurately answer customer inquiries about their security practices.

The Result

Zephyr Health passed their SOC2 certification within six months from start-to-finish — and with no qualified findings by their external auditors. Customers have reported they feel confident Zephyr Health takes their role as a data custodian seriously.

The Solution

Zephyr Health approached us to do a policy review and gap analysis against security certifications. Through our consultation process, we determined that the issue was customer-driven. Our analysis showed that the appropriate security framework for Zephyr Health would be the Service Organization Controls (SOC2).

> *"We continue to enjoy the benefits of the SOC2 implementation; thank you again for your help."*

WILLIAM KING, CEO, ZEPHYR HEALTH

SECURING A COMPETITIVE ADVANTAGE

CHANGE HEALTHCARE

Customer	Change Healthcare, Inc.
Website	changehealthcare.com
Industry	Healthcare Software Vendor
Services Provided	Application and source code security assessment

Summary

- Change Healthcare is a leading company in the healthcare industry, operating the largest financial and administrative information exchange in the United States.
- As their business expanded, we were there to help Change Healthcare grow and evolve their security posture.
- Over the years, we've learned and gained insight into Change Healthcare's business. As a result, we've been able to tailor our services to fit their unique needs.
- This nine-year partnership provided Bishop Fox the opportunity to help Change Healthcare grow and evolve in their security posture.

Scan the Qr code to access the case study

The Challenge

Change Healthcare connects more payers, providers, and vendors than any other healthcare business in the marketplace. With a network that encompasses more than 800,000 providers and over 1,200 government and commercial payers, protecting their customers' sensitive data and their security posture are top priority.

The Result

Our tailored services have helped place Change Healthcare ahead of leading competitors in their field. This nine-year and counting partnership continues to provide Bishop Fox the opportunity to help Change Healthcare evolve in their security posture.

The Solution

With application assessments and source code review, PCI compliance, incident response, training, and ongoing consulting, Bishop Fox works diligently to ensure that Change Healthcare's security concerns are addressed from every angle. Our teams have collaborated to address security issues and protect Change Healthcare's services.

> *"This level of security has set us apart from our competition and in many cases has been the deciding factor in winning competitive bid scenarios. I couldn't be happier with the results and the relationship that we've achieved together."*

ENGINEER AT CHANGE HEALTHCARE


BISHOP FOX
www.bishopfox.com
@bishopfox