How Hiring Hackers Can Make Your Institution Safer

cyber security data privacy

Summary: The average cost of a data breach in the finance industry is estimated to be $5.97MM. Increasingly, financial institutions are using so-called white hat hackers to test the security of their systems. We discuss how they can help you improve your cybersecurity and protect your CFI and customers.

The saying *"it takes a thief to catch a thief"* has some serious merit to it. From 2005 to 2007, the Discovery Channel took that advice to heart, producing "It Takes a Thief," a reality show where two ex-burglars, Matt Johnston and Jon Douglas Rainey, helped homeowners proof their homes against break-ins. In the episodes, Rainey would attempt to break into the homes and explain the vulnerabilities he found in their security while the owners watched from a remote location. Later, the ex-burglars would walk the homeowners through how to fix those security issues to make their homes more impervious to burglars.

The show's premise demonstrates that people who know how criminals operate can be a very useful resource to help prevent crime. As many financial organizations are discovering, the same logic can be applied to cybersecurity. Many skilled hackers are now using their expertise to help fight cybercrime. Known as "white hat" hackers or "ethical hackers", they are experts in cyber defense and can help make an organization's systems as secure as possible from attack by cybercriminals, or black hat hackers.

Cybersecurity: A Top Priority for CFIs

As finance and banking become increasingly digital, opportunities for cybercriminals continue to rise. A successful cyberattack can have far-reaching and severe consequences for a community financial institution (CFI) — from compromised critical customer data to considerable reputational damage. Given that the average cost of a data breach in the finance industry is now estimated at $5.97MM, CFIs also have a financial imperative to reduce their chances of being attacked.

With regulators prioritizing cybersecurity in their assessments of financial organizations, CFIs need to ensure they've turned over every stone, in an effort to protect their sensitive data and their customers. To that end, ethical hackers are becoming more commonplace within many financial institutions, as part of a holistic approach to cybersecurity. We discuss how white hat hackers can help you fight fraud and cybercrime, and the value they can bring to your institution.

How White Hat Hackers Can Help

While "black hat" hackers penetrate systems illegally for financial or other gains, white hat hackers have permission to do so to assess an organization's vulnerabilities. However, given the rise of artificial intelligence (AI) and sophisticated digital cybersecurity tools, some institutions may wonder if they really need white hat hackers. Why would you purposefully expose your system to potential external risk or human error? In response, as one cybersecurity company suggests, *"only a hacker can think like a hacker."*

To fully understand the strengths and weaknesses of their systems, institutions need people who can behave

like cybercriminals to test those systems. As such, white hat hackers can form an important component of a CFI's comprehensive approach to fighting cybercrime. Used alongside automated tools, vulnerability scanning, and AI-based programs, they can help counteract sophisticated cyberattacks.

Here are **three reasons** why you may want to consider using white hat hackers:

1. **New insights.** Ethical hackers can bring a fresh perspective to an institution's defenses. This allows them to uncover vulnerabilities, loopholes, and hidden issues more easily in your infrastructure. Using these insights, they can advise on how you should develop your cybersecurity toolsets and identify where to direct resources to stay ahead of new and developing threats.
2. **Real-world testing.** By simulating real-world hacking attacks, white hacks can assess how your infrastructure would hold up against an actual attack. This testing enables you to quickly respond to any identified weaknesses, customizing appropriate responses and emergency actions based on specific risk scenarios. This means your institution can be better able to implement measures and fix problems before any real damage is done.
3. **Reputational benefits.** Using ethical hackers to improve your cybersecurity will of course help your institution keep customer data and money safe. Communicating what you're doing to protect your customers should help improve your institution's trustworthiness and reputation.

Potential Limitations of White Hat Hacking

Although white hat hackers offer many benefits, there can also be downsides. Here are **three limitations** your institution should be aware of:

1. **Cost.** Hiring a company that offers white hat hacking services can be very expensive. Employing ethical hackers internally could also be costly, and it can be difficult to source the right talent. Fortunately, some companies offer a range of services to suit different budgets — from technology that provides automated vulnerability scanning to humans conducting penetration testing. Some financial institutions even engage ethical hackers through bug bounty programs, meaning they invite external white hats to test the security of their systems, offering rewards to those who discover vulnerabilities.
2. **Insufficient rigor.** Haphazard or insufficient testing methods can result in limited findings or a false sense of security, potentially compromising an institution's infrastructure. The use of white hats needs to be considered part of an extensive risk management plan and system.
3. **Potential exposure to third-party risks.** Humans are often one of the weakest links in cybersecurity. Unfortunately, using external resources always brings an increased risk of exposure to vulnerabilities — particularly if third-party service providers are not thoroughly vetted.

As CFIs continue to try to meet the fast-changing demands of the challenging cybersecurity landscape, you may want to consider the role of white hat hackers as part of your comprehensive cybersecurity program. By employing the services of people who can think and act like cybercriminals, you'll be better able to stay abreast of hacking trends, guard your system against threats, and protect both yourself and your customers.

WE HELP DE NOVO AND ESTABLISHED BANKS

PCBB not only has the expertise and services to successfully help launch new banks, but also the solutions to help them grow and succeed. Know someone interested in starting a bank? Refer them to us so they can get started right away.

ECONOMY & RATES

Rates As Of: 03/27/2023 01:19PM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	4.74	-0.14	0.32
6M	4.76	-0.41	0.00
1Y	4.48	-0.52	-0.22
2Y	4.01	-0.81	-0.42
5Y	3.61	-0.57	-0.39
10Y	3.54	-0.38	-0.34
30Y	3.77	-0.15	-0.20

FF Market	FF Disc	IORB
4.83	5.00	4.90

SOFR	Prime	OBFR
4.80	8.00	4.82