The benefits of operationalizing cybersecurity

How you can build a more robust cybersecurity program

WIPFLI

Overview

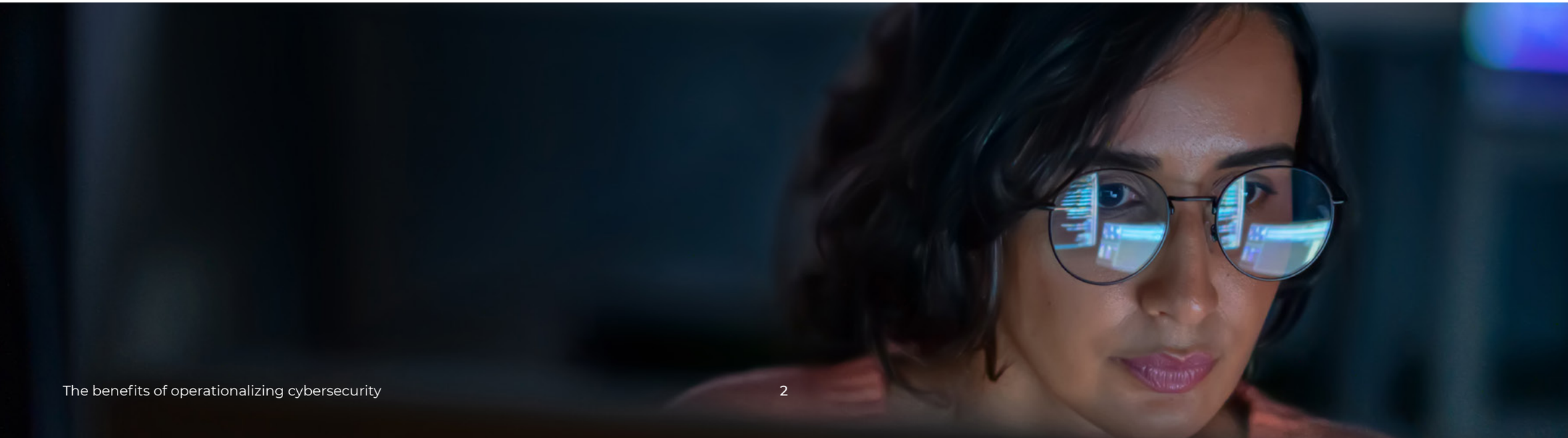
With the increasing prevalence and sophistication of cyberthreats, cybersecurity is now a top priority.

The consequences of a cyberattack on your organization can be far-reaching, including not just the costs of breach mitigation but also the damage to your reputation and loss of customer trust. Yet many organizations still view cybersecurity as a compliance checkbox they need to fill.

When you elevate cybersecurity from a regulatory requirement to an embedded part of your operations, you get the protection you need to secure customer data and adopt new innovations with confidence.

Discover how you can operationalize cybersecurity at your organization, including:

- The importance of adapting to modern cyberthreats.
- A guide for identifying and scheduling critical cybersecurity operations.



Making cybersecurity your priority

If your organization isn't prioritizing cybersecurity, it may be time to start.

Over 72% of businesses worldwide were affected by ransomware attacks in 2023 — the highest percentage reported in five years. And as organizations continue to face pressure to modernize and enhance digital engagement, securing data and systems is an increasingly critical concern.

Your financial institution also needs to consider:

1. The evolving threat landscape

With rapid technological advancements and the increasing reliance on digital platforms, organizations are facing increased threats from cybercriminals.

AI has accelerated these issues by giving hackers access to solutions that allow them to streamline their processes. For example, generative AI makes it easier for hackers to create phishing scams by making quality, convincing content more accessible. And hackers can even use AI to clone voices and target employees via phone calls.

Mobile device security has also become a growing concern for organizations as mobile or web customer platform use increases. Cybercriminals often target mobile devices through malware-infected apps or fake websites designed to steal user information. As more individuals rely on mobile access to services, protecting these devices from threats has become crucial for organizations.

2. The costs of a breach

The financial consequences of a cybersecurity breach can be significant. According to the 2024 IBM Cost of a Data Breach Report, the global average cost of a data breach is $4.88 million — up 10% from the previous year.

However, the reputational consequences can be even heavier.

Losing customer or stakeholder trust can cost your organization far more than just breach mitigation. A cyberattack erodes confidence in your organization, and you're not likely to recover your damaged brand reputation quickly.

Cybersecurity by the numbers

$4.88 million
The global average cost of a data breach, according to IBM.

$3.4 billion
The number of spam emails estimated to be sent every day.

$568,000
The average ransomware payment in Q4 2023.

Operationalizing cybersecurity at your institution

For many organizations, cybersecurity is a yearly activity focused on performing regulatory requirements, such as penetration testing, security assessments and revisiting your information security program.

However, cybersecurity shouldn't just be a once-a-year activity. It should be built into your operations, with ongoing monitoring and processes that help ensure you're staying secure.

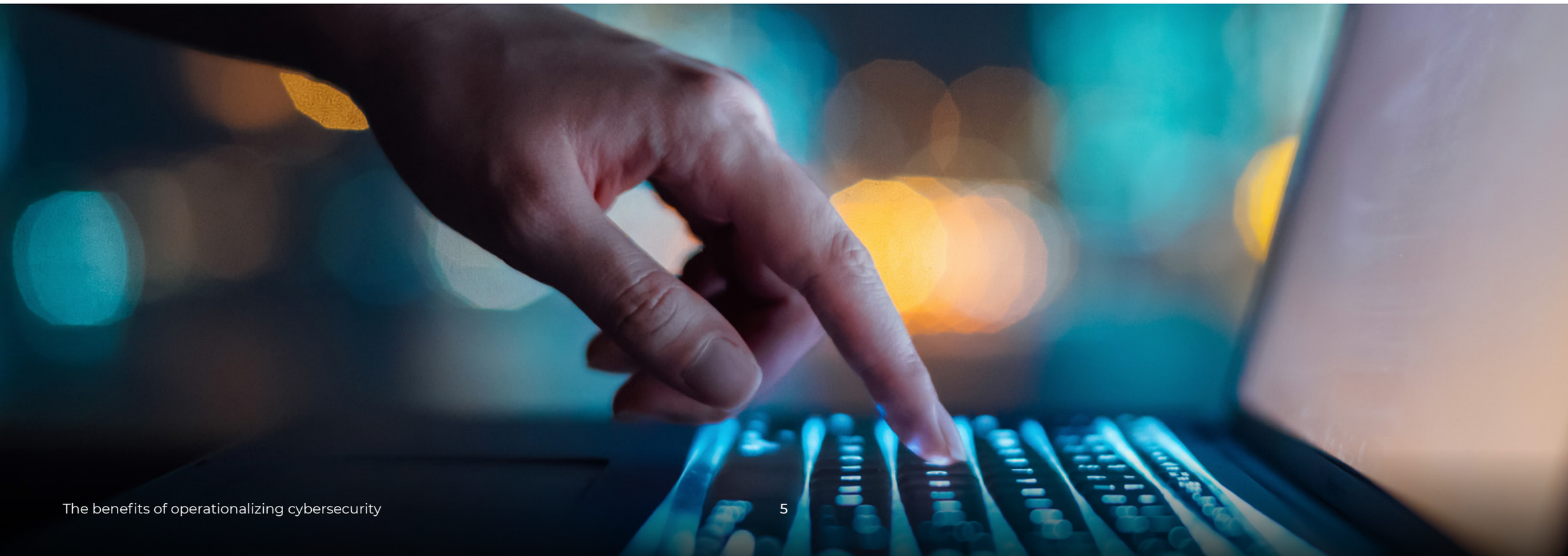
By operationalizing cybersecurity, your organization is better positioned to keep pace with rising cyberthreats and stay secure as you modernize and improve your digital customer experience.

1. Building your cybersecurity program

Operationalizing cybersecurity starts with a program that identifies the key operations you need to perform and at what frequency.

Your leadership will need to consider:

- **What are we doing daily to be proactive about monitoring our environment?**
  24/7 monitoring and taking measures such as reviewing your security logs for anomalies can help you identify indicators of compromise faster and reduce the time attackers have in your systems if they gain access.
- **What are we doing weekly or monthly to maintain our security?**
  Regularly evaluating key security functions — such as access control, privileges and permissions — updating policies, performing vulnerability testing and conducting employee education can help you manage risks and stay on top of the latest threats.
- **What are we doing quarterly or annually to improve our cybersecurity program?**
  In addition to meeting your yearly regulatory requirements, it's also important to evaluate and enhance your cybersecurity operations at the leadership level, including conducting drills, to help ensure that your program remains effective.



Cybersecurity program guide

You can use the following guide as a template to help you develop your program:

Daily operations

- Monitor security events and alerts.
- Review security logs for anomalies.
- Deploy patch management and updates for critical systems.

Weekly operations

- Review threat intelligence reports.
- Review access controls and privileges.
- Ensure offboarding is occurring in a timely manner.

Monthly operations

- Audit access control.
- Complete a test restoration of a file or folder.
- Conduct perimeter and internal vulnerability scanning.
- Conduct email phishing tests.
- Create a security operations report on key metrics.

Quarterly operations

- Host employee cybersecurity training sessions.
- Conduct security incident response drills.
- Conduct penetration testing/vulnerability assessments.
- Change passwords for administrative accounts.
- Audit firewall, network device and endpoint configurations.
- Review data and device management and destruction activities.
- Conduct pretext calling social engineering to validate that client authentication procedures are followed.
- Review incident response plans and business continuity plans.
- Conduct risk assessments and management reviews.

Annual operations

- Conduct red team exercises to simulate cyberattacks.
- Conduct a full-scale cybersecurity tabletop exercise involving key stakeholders.
- Test your disaster recovery plan.
- Review and update the entire cybersecurity program.
- Conduct cybersecurity maturity model assessments and benchmarking.
- Manage vendor risk.
- Establish board reporting and get security program approval.

Take your cybersecurity operations further with Wipfli.

A security breach can damage customer trust, interrupt workflows, destroy data and harm your organization's reputation.

To effectively manage your cybersecurity risk, it's crucial to identify and understand potential threats. This requires not only the right tools and systems but also a comprehensive strategy that integrates security into your operations.

Wipfli can help you enhance your cybersecurity program with proactive, experienced guidance. From threat analysis and simulations to round-the-clock monitoring and data recovery, our team can help safeguard your organization by applying the latest solutions to meet evolving threats.

We can help bridge the gap between your operations and technology with scalable support for:

- Cybersecurity health checks
- Threat and vulnerability assessments
- Attack simulation
- Business continuity and incident response
- Virtual CISO services
- Managed security services
- Industry-specific compliance solutions

Visit our site to learn more about how Wipfli can help you build a stronger cybersecurity program.

wipfli.com