EBOOK

The cost and ROI of cybersecurity

imprivata®

It’s the dreaded question every CISO hears from their CFO: “What’s the ROI on cybersecurity?”

Data breaches are costly. The average cost of a data breach is $4.35 million—a lot of money considering just about every organization has been breached, doesn’t know they’ve been breached, or is going to get breached at some point.

So when it comes to investing in cybersecurity, the money put in is well worth the cost savings. But how can you tangibly articulate the cost savings and ROI on investing in cybersecurity solutions?

Measuring the success of cybersecurity solutions is challenging. For teams like marketing and sales, calculating ROI is a simple math equation: what’s the difference between what you spend and the revenue you make from that expense?

Cybersecurity is a different kind of outcome to quantify. It’s not based on hard numbers like revenue and profit, and many times, the success or outcomes of cybersecurity efforts are invisible, like the number of data breaches that haven’t happened, or the amount of time saved on resolving cyber incidents.

As difficult as they might be to quantify, those metrics are important indicators in measuring the security of an organization. If those numbers aren’t compelling, it could cost your company millions.

The challenges in investing in cybersecurity and calculating ROI

- **The return on cybersecurity is hard to calculate.** As mentioned before, there are fewer straightforward metrics or methods to determine the ROI on a cybersecurity investment. If you can't justify the purchase with a lucrative outcome, decision-makers are less likely to invest.

- **There's often misalignment between IT and security and the executive team.** There's a common misconception that security professionals don't know the business objectives of a company. This narrative only makes the conversation between a CISO and a CFO that much more difficult. However, there has been a shift in the C-suite lately—senior leadership is seeing cybersecurity as a business issue rather than just an IT issue. While this isn't happening at every organization, board-level members are starting to understand how cybersecurity can prevent reputation damage, loss of customers, and consequences of downtime.

- **Businesses don't think they need cybersecurity.** The biggest culprit of a cyberattack on an unsecured company isn't the bad actor—it's the "it won't happen to me" mentality. Organizations tend to think if they haven't had any cyber incidents so far, it probably won't happen to them. This lie is costing companies millions, and doing nothing in regard to cybersecurity is doing a lot of damage.

- **IT and security teams don't know what's needed.** There's a lot of buzz around cybersecurity terms like "Zero Trust," "cybersecurity mesh," and "decentralization." These words aren't meant to scare—they're meant to warn and protect. Cybersecurity frameworks are trending towards remote, perimeter-less security methods that involve multiple levels of control. This means the digital landscape is changing and security methods need to evolve with it. But with so much change, it's hard to keep up with the best practices of cybersecurity and what companies should purchase to make it worth the investment.

THE COST OF A CYBERATTACK

$4.35 million

IBM found that the average cost of a data breach is $4.35 million.

$4.54 million

The average cost of a ransomware attack is $4.54 million—not including the cost of the ransom.

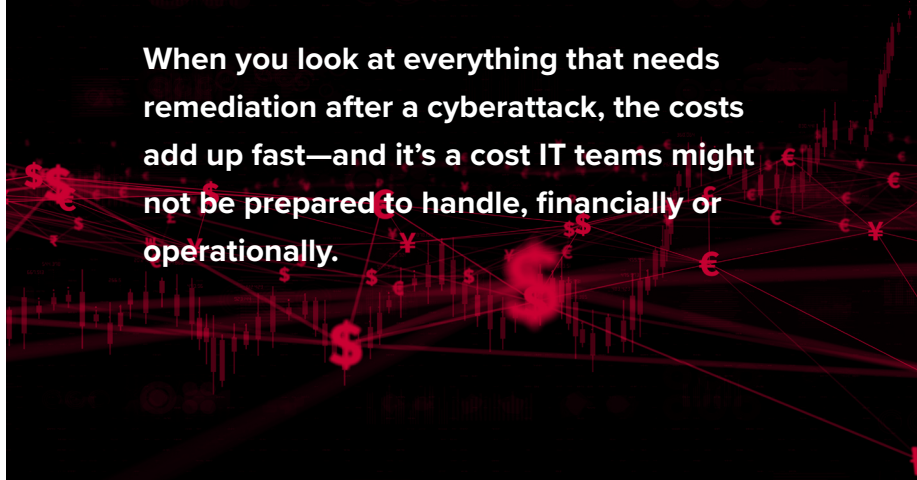
$9 million

In the United States, it takes approximately $9 million to remediate the impacts of a cyberattack—the highest of any country.

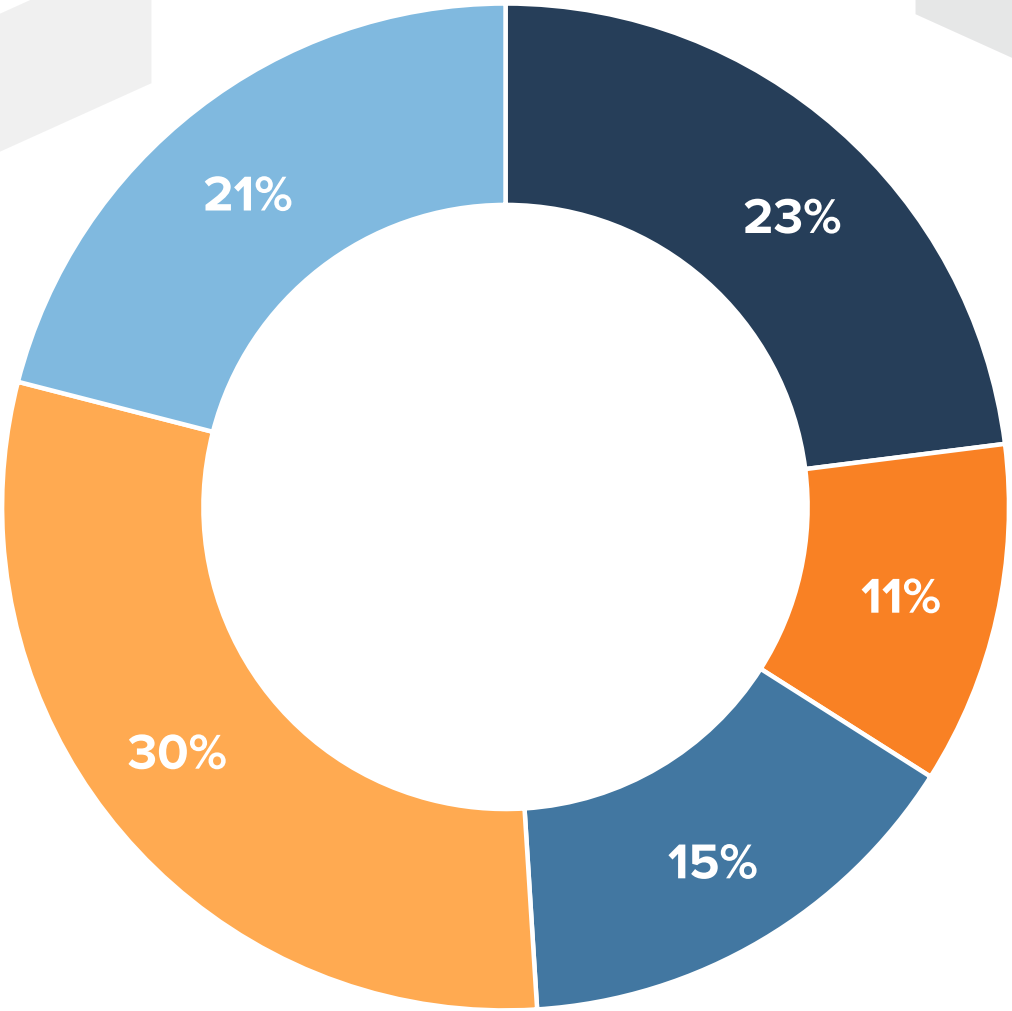
277 days

It takes an average of 277 days to identify and contain data breaches.

When you look at everything that needs remediation after a cyberattack, the costs add up fast—and it's a cost IT teams might not be prepared to handle, financially or operationally.



How much of total cyberattack clean-up cost goes to different areas:



- Remediation and technical support activities, including forensic investigations, incident response activities, help desk and customer service operations
- Users' idle time and lost productivity because of downtime or system performance delays
- Disruption to normal operations because of system availability
- Damage or theft of IT assets and infrastructure
- Reputation loss and brand damage

COSTS OF A CYBERATTACK BY INDUSTRY

Critical Infrastructure
$4.82 million

Education
$3.86 million

Healthcare
$10.10 million

Retail
$3.28 million

Financial services
$5.97 million

Public sector
$2.07 million

Energy
$4.72 million

It doesn't matter how big your budget is or what industry you're in. Cyberattacks are costly. Even if a company has sizable IT and cybersecurity budgets, it's doubtful that $5 million is set aside as an "in the case of a cyberattack" fund. The only option is to invest upfront to proactively stop these attacks—and subsequent costs—from occurring.

The downward spiral of a cyberattack

How much cybersecurity costs

Cybersecurity products will vary from vendor to vendor, but on average, organizations are spending 22% of their IT budgets on cybersecurity. In our opinion, this isn't enough.

Despite this investment, cybersecurity is still average at best. Over half of organizations are still experiencing cyberattacks. The rate of attacks and ransomware are only increasing, which means cyber criminals aren't afraid of cybersecurity defenses. And they shouldn't be, especially considering 59% aren't deploying strategies like Zero Trust, which is built to detect, prevent, and mitigate threats.

Automation and streamlining security technology can save organizations financially and operationally. The investment upfront, no matter how heavy, will prove its worth when previously manual or siloed workflows are streamlined and there are substantial cost savings involved if/when a cyberattack happens.

- $3.05 million
    - Companies with fully deployed artificial intelligence and automation incurred costs that were $3.05 million lower than the average cost of a breach.
        - Automation: artificial intelligence (AI), machine learning, analytics, automated security orchestration, extended detection and response (XDR)
- $2.66 million
    - Organizations that have incident response teams and tested incident response plans saved $2.66 million on the average cost of a data breach.
- $2.10 million
    - Risk quantification techniques saved organizations over $2 million on average data breach costs versus organizations that did not deploy risk quantification.
- $1.51 million
    - On average, companies that have a mature Zero Trust deployment saved $1.51 million compared to those that have early adoptions of Zero Trust.
- $550,000
    - Remember, employees are part of the cybersecurity budget. Organizations with sufficiently staffed teams saved over half a million in data breach costs versus those whose teams are insufficiently staffed. Personnel is also an investment worth making.

Shorter data breach lifecycles are associated with an overall lower data breach cost. Automated technologies and processes reduce the mean times to identify and contain data breaches—and subsequently, reduce data breach costs (or prevent the data breach altogether).

How to calculate cybersecurity ROI

Calculating ROI on a cybersecurity investment doesn't have to be complicated. There are multiple ways to calculate the ROI with metrics some of your technology might already track.

- Use network monitoring to log and view attempted (and prevented) attacks
    - Some cybersecurity technology offers monitoring capabilities that let you see attempted hacks. If you have this information:
        - # of attempted hacks x the average cost of a breach
    - Then compare the cost of cybersecurity investments versus the cost of the potential attacks.
- Calculate the cost of downtime and compare to the cybersecurity spend to find the ROI on isolated incidents.
    - Determine the number of days your business would lose if it got hacked.
    - Then figure out how much money you'd lose due to the downtime.
        - Cost of lost productivity
        - Impact of customer revenue
        - Lost production or billed services
    - Add on top of that the time and money spent recovering data loss and repairing damaged infrastructure.
    - Compare that to the amount of money you'd spend on security technology.
- Determine which compliance regulations you'd violate if your company experienced a security breach and the average fine for those types of violations. The fines and penalties alone could be worth more than the cybersecurity investments.
- Calculate the cost savings on ongoing costs, such as software licenses, storage spaces, vendors, etc.
    - Automation can save money by streamlining multiple processes or cutting down on resources
- Assess the value of your most critical assets. Determine how much it would cost to recover those assets vs. the investment to protect them with cybersecurity systems.
- Calculate any efficiency gains as it relates to time spent. Take the amount of time spent in manual processes and multiply it by the salary or hourly rate of an employee (or vendor). Then compare that price to the automated solution.

METRICS FOR MEASURING CYBERSECURITY ROI

- Time savings
- Cost savings
- Reduced risk of a breach
- Compliance
- Incident management metrics:
    - Mean time to detection or identification
        - The average time between the beginning of a security incident and when a security team discovers it
    - Mean time to respond
        - The average amount of time it takes to take action after discovering an incident and resolving any issues
    - Mean time to patch
        - The average amount of time to fix the vulnerabilities that caused a security incident
    - Mean time to recover
        - The average time it takes to recover systems from attack damage, from the moment the impact hits to when systems become operational again
    - Mean time to resolution
        - The average time it takes to fully resolve a security incident, including implementing preventative measures post-hack
    - Mean time to contain
        - The average amount of time between detecting an incident, resolving the incident, and preventing any further implications of the incident

Things to consider

One of the greatest difficulties for cybersecurity leaders is getting funding for cybersecurity initiatives. IT budgets tend to be hefty—after all, technology is what keeps businesses running, and technology is expensive. But when cybersecurity asks for more than the average 22% they're allocated out of a multi-million dollar budget, decision-makers are hesitant.

IT expenses include costly items like equipment, software, applications, and personnel. Some might see any additional cybersecurity investments as peripheral rather than essential. Keeping some additional things in mind—and bringing them to the forefront of the conversation with decision-makers—will emphasize the importance and urgency of cybersecurity investments.

- Cyberattackers come from all angles.
    - Third-party remote access is one of the most common attack vectors. Data breaches caused by a third-party cost $370,000 more than the average cyberattack. Access given to external users needs to be granularly controlled to prevent bad actors looking to compromise vendor privileged access.
    - Let's not forget about internal threats. Cybersecurity is no longer just about keeping bad guys out—it's also about making sure those on the inside aren't abusing privileged access, compromising systems, or stealing data.
- Data breaches DO impact business reputation.
    - 19% of customers say they would abandon a retailer that's experienced a data breach. That's potentially a 19% revenue loss.

- Digitization is inevitable. More access points means more points of vulnerability.
    - Between the cloud, remote workforces, and off-premise servers, businesses are going digital. And it's not a bad thing. In fact, it's great for businesses to be more accessible for their customers and employees. But if you're going to digitize, you need to have the security to back it up. Data breaches associated with remote workers are more expensive. More importantly, your customers trust you to take care of their data that you're moving from an on-premise server room to the cloud. And your employees trust you to protect their digital identities and credentials that lead to critical assets and access points.

If you calculate the ROI on cybersecurity, you'll find it's worth the investment. Strong cybersecurity practices involve proactive approaches and thorough assessments of the access points, identities, and assets that need protecting. Take the time to understand your cybersecurity needs, then make the decisions that could save your company from a downward spiral of post-cyberattack implications.

Contact us to learn more about the ROI on Imprivata's cybersecurity solutions.

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

786-2023_ebook_cost-and-roi-of-cybersecurity