501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC

THE ROI OF A FRACTIONAL CISO

Sound business decisions are based upon an understanding of the financial ROI expected from the investment. Engaging a fractional CISO is no different. 501CISO is designed to be a low-cost, high return on investment service that leverages cybersecurity expertise to minimize the costs and risks associated with cybersecurity incidents.

501CISO is a low-cost, high return-on-investment service that leverages cybersecurity expertise to minimize the risks and associated costs of cybersecurity incidents.

FRACTIONAL CISO VALUE

Reporting & Executive Management Communication: Developing reports, presenting, and advising top executive management on all security matters.

Risk Assessment: Perform a risk assessment to understand the overall vulnerability of any particular asset within the organization.

Strategic Security Roadmap: Develop a roadmap and budget with sized, sequenced, and prioritized initiatives.

Quantify Cyber Risk Improvements: Utilize data-driven reports to quantify an organization's improvement in their cyber-risk position.

Risk Management Program: Evaluate and advise on new security threats while maintaining a risk register and corrective actions plan.

Regulatory Compliance & Audits: Document high level requirements for compliance and assure that strategic goals are implemented within a controlled, secure framework.

Vendor Management: Manage and provide oversight of vendors and lead the associated due diligence.

Development and Implementation of Critical Security Policies and Procedures: Development and adherence to security policies and procedures.

Asset Assessment: Classify hardware and software assets based on their criticality and business value.

Security Architecture: Review security architecture for new projects and applications.

Awareness & Training: Maintain/update/provide training and awareness plan and materials.

Incident management: Manage, communicate, and coordinate a response to security event/incidents.

Privacy Law Compliance: Develop and implement policies and procedures to maintain compliance with GDPR and U.S.-based privacy laws.

501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC

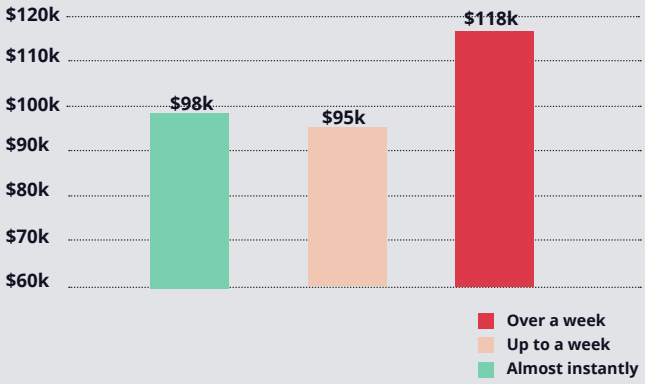
CYBER INCIDENT COSTS

Operational Downtime: *Organizations will have unique hourly costs for operational downtime. The average downtime of a ransomware attack in 2021 was 20 days. AAt any daily cost, this is a significant operational expense.*

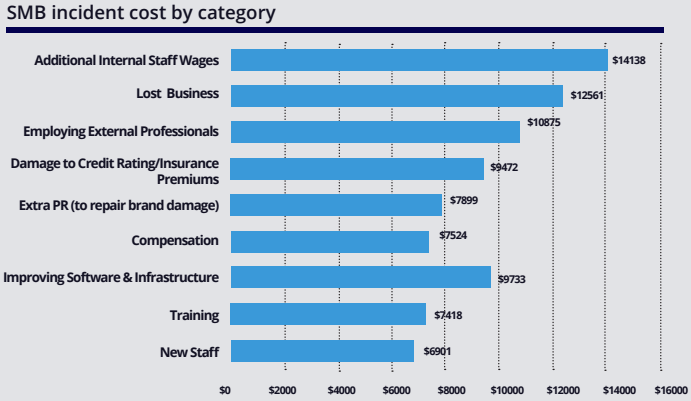
Incident Remediation Costs: *Incident response specialist costs vary, but typically start at $500/hour. Two specialists working for the average 20-day window equates to $160,000.*

Regulatory Fines: *The GDPR and CCPA are great examples of how regulatory fines can quickly add significant costs on top of an already expensive situation, with potential fines ranging from $7,500 to millions of dollars.*

When data breaches were discovered and how much they cost SMBs



SMB incident cost by category



Legal Fees: *Most businesses retain counsel as a best practice when triaging a cybersecurity incident. While hourly attorney rates vary case-by-case, they tend to hover around $1000/hour.*

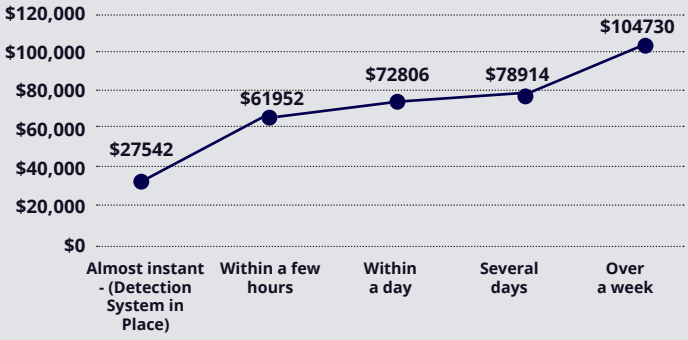
Devaluation of Trade/Brand Name: *Devaluation of trade name is an intangible cost category referring to the loss in value of the names, marks, or symbols an organization uses to distinguish its products and services.*

Insurance Premium Increases: *It is not uncommon for a policyholder to face a 200% increase in premiums for the same coverage, or possibly even be denied coverage until stringent conditions are met following a cyber incident.*

Lost Value of Customer Relationships: *Organization that have quantified the value of each member or customer can calculate total loss by assuming some percentage of lost customers or lost customer opportunities.*

Loss of Intellectual Property: *Loss of IP is an intangible cost associated with loss of exclusive control over trade secrets, copyrights, investment plans, and other proprietary information that can lead to loss of competitive advantage, loss of revenue, and lasting and potentially irreparable economic damage to the organization.*

Cost of recovery vs. time needed to discover a security breach for SMBs



Making every reasonable effort to avoid a cyber incident is the wisest business strategy. The costs of fractional CISO leadership and enhanced cyber protections are a fraction of the total incident costs.

To begin, contact: **info@501ciso.com**