RETHINKING Cyber Risk

Why ‘cyber risk quantification’ is crucial to calibrating sound security investment decisions as cyberattacks shift to social engineering. Plus four economic benefits for shifting to human-centric cyber strategies.

By Scoop News Group

The digital operations of government agencies nationwide stand as a vital foundation of public service. Protecting that foundation against security risks, however, calls for a fundamentally different investment calculation. Decision-makers need to weigh the value of cybersecurity software and infrastructure investments against the potential costs of cyberattacks.

At a time when AI-enabled and human-centered cyberattacks are escalating dramatically, it's increasingly important to recognize this distinction as agency officials grapple with how and where to allocate scarce budget dollars.

The new budget reality:
Federal and state government agencies are confronting a stark new reality as long-standing federal support for cybersecurity information sharing and infrastructure investments has been cut dramatically by White House officials.

- **Staffing and budget** cutbacks**:** The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is reducing resources dedicated to national threat intelligence that corporations, government agencies and critical infrastructure providers depend on.

- **Compounding concerns:** State security officials are now scrambling in response to federal funding cuts to MS-ISAC, the Multi-State Information Sharing and Analysis Center, which has been crucial in helping state security officials stay ahead of cyber threats for the past 20 years. The cuts will likely force state officials to become more self-reliant and require new strategies to manage cyber risks.

Shifting threats:
Government agencies continue to confront mounting cybersecurity challenges as threat actors exploit AI-enabled tools and impersonation techniques to access sensitive personal, tax, and health data. The cost and disruption of data breaches and ransomware attacks can impact agencies for months while leaving lasting and incalculable reputational and political damage.

- "**Data security** is a significant issue as more of the burden to protect constituent data is shifting towards states and localities," says **Ryan Witt**, vice president of industry solutions at Proofpoint. "Clearly, there's going to be less funding, leaving states more on their own to protect themselves. There will not be as much guidance coming from the federal government."

- **That will place new demands on state CISOs** whose responsibilities continue to grow in proportion to the expanding attack surface, according to a recent Deloitte-NASCIO Cybersecurity Study.

Reassessing the risk equation:
This new reality is forcing difficult decisions between chief financial, information, and security officers as they weigh the value of cybersecurity investments against the potential costs of cybersecurity threats, says **Marcel Eisma**, senior director, value management office at Proofpoint.

- **Defining risk:** "Most organizations still struggle to define risk coherently," says Eisma. Traditional ROI is based on predictable income or productivity gains over time from an investment. "Return on security investment (ROSI) is different — it's based on cost avoidance, which is extremely unpredictable."

- **Quantifying risk:** To better gauge the financial impacts of risk, "more and more organizations are jumping on the 'cyber risk quantification bus' — because how do you quantify the value of something that does not happen?"

> "Clearly, there's going to be less funding, leaving states more on their own to protect themselves. There will not be as much guidance coming from the federal government."
>
> – Ryan Witt, vice president of industry solutions at Proofpoint

Cyber Risk Quantification (CRQ) is a framework that addresses that question, using methodologies like OpenFAIR — Factor Analysis of Information Risk — to determine in dollar terms, "what's the likely frequency of something happening and the likely magnitude of that happening?" explains Eisma, who is a FAIR-certified analyst. OpenFAIR also provides a common language for risk professionals.

- **The car accident analogy:** Eisma likens the financial exercise to calculating the value of "not getting into a car accident yesterday or the past year. That's good news. How much did that save you?" By translating probabilities and impacts into monetary values, agencies can compare cybersecurity decisions on equal footing with other budgetary priorities. It also helps agencies "put a number on the risk that they are buying down by going with option A, B, or C offered by vendors," he says.

- **Moving beyond red-yellow-green:** A second reason to embrace risk quantification is the challenge of translating red-yellow-green risk matrices into meaningful or comparable priorities. "Are two yellows better than a red? You can't subtract a green from a yellow and then add a red — you need dollar numbers," Eisma argues. Risk quantification also supports conversations around political capital, multi-year budgets, and federal grant eligibility, he adds, by providing a mathematical foundation for more objective decision-making.

The new trajectory of risk:
Chief financial and risk officers must also recognize how the risk environment is evolving as threat actors have more tools, data, and AI at their disposal. While the vast amount of personal and sensitive data held by government agencies has always made them a prime target, it's becoming easier for threat actors to bypass traditional cyber defenses. As a result, it's increasingly important for agency officials to select their cyber investments carefully.

ROSI vs. ROI:
Why Security Economics Operate Differently

ROSI (Return on Security Investment)	Traditional ROI (Return on Investment)
Based on *cost avoidance* — reducing the probability and impact of adverse events (e.g., data breach, ransomware).	Based on *predictable income or productivity gains* from an investment (e.g., new factory, software platform).
Outcomes are inherently uncertain — risk events may never occur or could happen multiple times in short succession.	Outcomes can be forecast within tight margins using production and revenue data.
Value is realized through *loss prevention, risk mitigation,* and *resilience improvement.*	Value is realized through profit generation.
EXAMPLE: A cyber investment may reduce the likelihood of a multimillion-dollar breach — but the "savings" are probabilistic, not guaranteed.	EXAMPLE: A factory investment yields a 10% profit margin on 100,000 cars per year.

THE SHIFTING CYBER THREAT LANDSCAPE

Traditional cybersecurity spending has long focused on fortifying network perimeters with firewalls and intrusion detection systems. While these remain essential, the lion's share of threat activity has shifted decisively towards compromising individuals through social engineering, phishing, application-based email exploits, and other human-centric tactics.

- **The latest figures** from Verizon's 2025 Data Breach Investigation Report (DBIR) show that out of 12,195 data breaches investigated by the DBIR last year, 60% involved human interaction. Credential abuse and social engineering tactics, such as phishing, were identified as the leading causes, far surpassing system vulnerability exploits, which increased last year but still accounted for only 20% of breaches.

Modern cyberattacks are rarely singular events but multi-stage, human-centric campaigns. Attackers initiate contact through one channel — a deceptive phishing email, for instance — and then escalate their efforts by harvesting credentials, compromising accounts, and moving laterally through internal systems or supply chain connections.

- **The rapid spread of the digital workspace**, along with the adoption of a multitude of collaboration tools such as email, social media, chat, and collaboration platforms like Teams and Slack, as well as file-sharing services, has significantly increased the attack surface, according to Witt.

- **Historically, cybersecurity was viewed as** "being good stewards of data," and an "insurance component" against reputational harm. Now, due to the increasing number of high-profile cybersecurity events, "organizations recognize that these events can essentially stop them from fulfilling their mission," he says.

> Risk is a dollar number that says, what's the *probability* of something happening and the *likely magnitude* of that happening?"
>
> – Marcel Eisma, senior director, value management office at Proofpoint.

One often-overlooked vulnerability is the exploitation of application email. Employees are accustomed to receiving email notifications from enterprise software applications such as those for financial and HR management, travel expenses, customer relations, or healthcare services (like Workday, SAP Concur, Salesforce, or Epic). Attackers are increasingly mimicking these emails to compromise employees' credentials and gain deeper access to network systems, says Witt.

- **Application notification emails** often lack the robust security features built into standard enterprise email systems, or bypass existing detection systems, Witt explains. Organizations are left vulnerable to these evolving threats without a comprehensive, multi-channel defense to intercept these communications.

THE ECONOMIC BENEFITS OF HUMAN-CENTRIC SECURITY

Shifting to a human-centric defense strategy involves rethinking an agency's approach to cybersecurity and embracing holistic systems that yield a more granular and comprehensive understanding of users' actions — and the context of those actions — across multiple channels. That's especially true, as traditional identity verification practices no longer offer the same level of protection they once did in stopping impersonators from breaching agency systems.

The payoff for agency CFOs:
Enterprise Strategy Group (ESG) analyzed how organizations profit from embracing human-centric cybersecurity protection systems, such as Proofpoint Prime, which is now used by more than eight in 10 Fortune 100 companies. Their results reveal **four key areas** where agencies can expect to see a significant return on their security investments:

01 Risk Alleviation:

Breaches caused by human error — including employees falling for phishing, impersonation attempts and malicious URLs attacks, as well as account takeover attempts — remain the top cause of security incidents. By reducing this human attack surface, ESG reported organizations experienced:

- **Fewer high-impact incidents,** such as data breaches, compliance failures, and reputational fallout.
- **Rapid containment and recovery from account compromise.** Real-time alerts, click-time URL protection, and automated quarantining of suspicious messages, powered by the latest technology, reduce phishing clicks by 82%.
- **Fewer productivity disruptions** and false positives from everyday threats like spam and generic phishing attempts, which generate unnecessary IT overhead.

02 Improved IT Workforce Efficiency:

Security teams are already stretched thin. Most operate under immense pressure in the face of growing volumes of human-targeted threats. Agencies can lighten this load by consolidating tools, automating manual tasks, and eliminating context switching. This leads to significant time savings and greater productivity in four key areas:

- **Admin and tool maintenance efficiency:** A consolidated platform simplifies administration by integrating multi-channel threat and impersonation protection, multi-stage attack detection, and human risk-based guidance and education.
- **Time saved triaging incidents:** Agencies also gain time and insights from pre-correlated, high-fidelity alerts enriched with contextual insights.
- **Time saved investigating incidents:** A centralized incident dashboard provides security leaders with complete visibility into the origin of threats, timelines, and impacted users. It enables teams to trace attack campaigns and verify user interactions within a single interface.
- **Time saved remediating incidents:** Security officials can respond faster to incidents by using streamlined containment tools and automated remediation playbooks to retract emails, lock user accounts, or enforce training modules directly from the incident console.

03 IT Optimization:

By retiring redundant point solutions and avoiding future spending on overlapping functionality, IT departments can expect reduced total costs.

- **Cost avoidance**: When the robust features of a modern, purpose-built, configurable platform are leveraged, there's a reduced need for higher-cost enterprise productivity and security bundles. That can lower the total cost of ownership by up to 40% compared to a legacy tech stack.

04 Improved Business Agility:

By consolidating multiple point solutions into a single platform, incident response workflows can be streamlined and the time spent on maintaining redundant infrastructure can be reduced. As a result, agencies can reinvest their time and resources into more valuable, forward-looking initiatives.

The bottom line:
"We have a very strong understanding of the types of human-centric threats agencies face, where threat activity is most likely to occur based on people's roles within an organization, the type of work they do, and the type of data they're interacting with," says Witt. "As threat actors continue to leverage AI to scale their attacks, the economic case for comprehensive cybersecurity for federal, state, and local governments has become even clearer and more compelling."

At the same time, it's more important than ever that agency leaders align on common assumptions around cybersecurity. When leaders share metrics and are transparent about the logic behind their choices, there can be meaningful comparisons across cyber investments. Ultimately, this helps them to better protect their employees, constituents, and data.

Learn more about how Proofpoint is empowering government agencies to gain an upper hand in combating human-centric cyber threats.

This article was produced by Scoop News Group for StateScoop and sponsored by Proofpoint.

STATESCOOP proofpoint.

See Side Bar on Next Page

A new era of cyber risk for government

The cyber threat landscape is changing rapidly for government agencies as malicious actors discover new methods to bypass traditional security defenses and exploit human vulnerabilities through the daily flood of emails, text messages, and social media posts.

A new analysis, based on data from Proofpoint's Nexus® threat intelligence platform, collected between May 1, 2024, and May 1, 2025, highlights the growing need for multi-layered, AI-driven detection as well as a comprehensive security strategy that focuses on protecting people across all digital channels — email, messaging, SaaS apps, and collaboration tools. Among the key findings:

URLs are now the primary vector for malicious attacks, surpassing email attachments:

4x

URLs are used 4x more often in malicious emails than attachments. This means employees are far more likely to encounter a malicious link than an infected file. This underscores attackers' relentless focus on credential harvesting, which can lead to account takeovers and deep network penetrations within government systems.

Mobile and emerging threat vectors are rising, expanding the attack surface beyond traditional email:

55%

of suspected SMS phishing ("smishing") messages contained malicious URLs.

75%

of organizations reported experiencing smishing attacks. Government employees, who heavily rely on mobile devices for communication, are becoming increasingly vulnerable to these urgent, emotionally driven mobile scams.

4.2 Million

QR code threats were were identified in the first half of 2025. QR codes are a new and dangerous vector. These attacks bypass traditional email filters and redirect users to phishing pages that are designed to steal credentials and sensitive data.

Social engineering attacks have grown more sophisticated and are designed to exploit human psychology to bypass security awareness:

- **Phishing kits, such as CoGUI and Darcula**, enable even less technically skilled criminals to launch high-volume, convincing campaigns that often impersonate well-known brands or government entities. Darcula, for instance, is frequently used in smishing campaigns that impersonate government services (e.g., road toll scams), directly targeting public servants.
- **Fake login pages and malicious URLs** are indistinguishable from legitimate ones, especially when generated using AI tools. This makes them incredibly difficult for employees to identify.

Malware diversification and remote access: Beyond direct data theft, attackers are establishing persistent access:

- **ClickFix URL-based malware**vcampaigns increased nearly 400% year over year. These threats often using fake CAPTCHA or error messages to trick users into running malicious content.
- **One-third of URL-based malware campaigns** delivered remote access software (RMM/RAS). While these are legitimate IT tools, threat actors abuse them to gain control of victim endpoints, exfiltrate data, and install ransomware. This could grant persistent, unauthorized access to government networks.

Source: Proofpoint's "The Human Factor 2025" Vol. 2, based on an analysis of 3.4 trillion email messages, 21 trillion URLs, 800 billion attachments, and 1.4 trillion suspicious SMS messages.