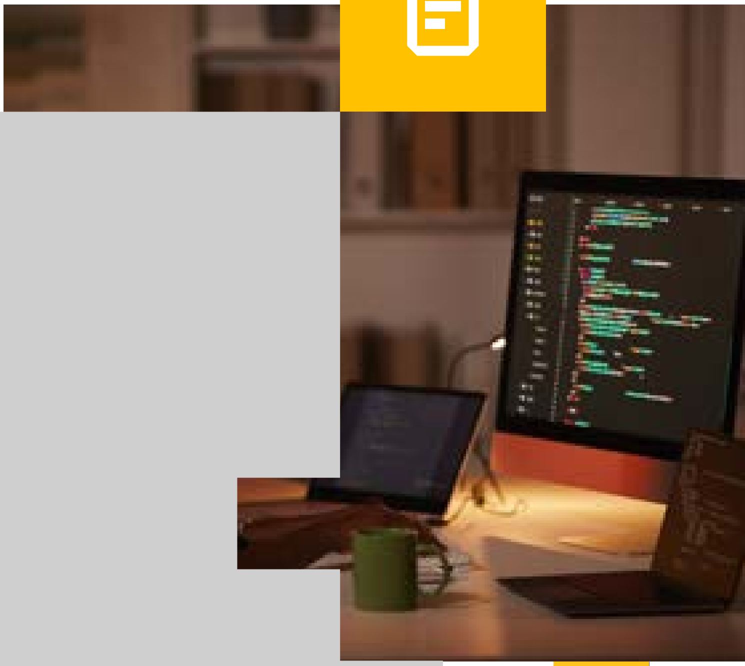
exabeam TUCANA CYBER SECURITY SOLUTIONS



White Paper

The Responsibility of Risk

Maintaining Cyber Risk Compliance Amid Growing State and Federal Regulations

Background

If there is a lesson to be learned from the onslaught of cyberattacks that have occurred in the year 2021, it is that no organization has immunity from becoming a victim of attack.

The crisis in the United States has become so severe that President Joe Biden has plead with the private sector to help. Other governments are taking legislative actions as well.

This led to the announcement that some of the United State's leading tech companies are committing billions of dollars to be invested over the next several years to strengthen cybersecurity defenses and to train workers.

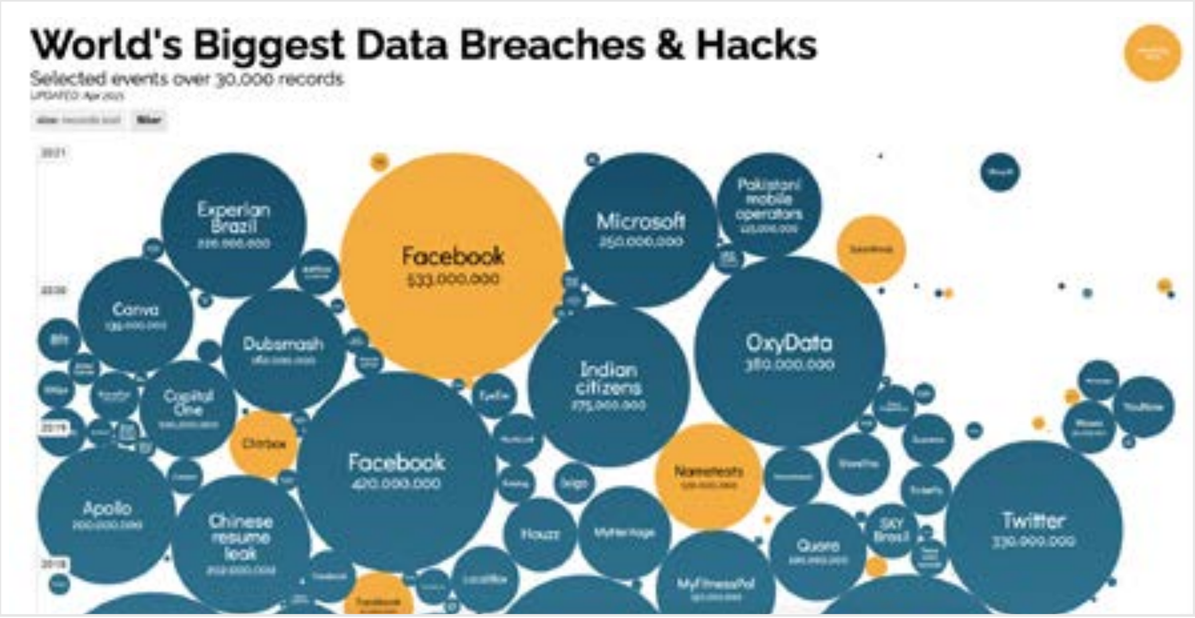


Figure 1 - Image courtesy of informationisbeautfiul.net

Big tech commits to help

In the United States, rivals Microsoft and Google are leading the way with $10 billion and $20 billion contributions, respectively.

Google's investments will focus on safeguarding supply chains and expanding zero-trust programs. This is welcomed news to the many companies and government agencies caught up in the SolarWinds attacks carried out earlier this year – a hack believed to be Russian state-sponsored.

Meanwhile, Microsoft specifically earmarked $150 million in technical services to help federal, state, and local governments upgrade their defenses. Something desperately needed as highlighted by cyberattacks throughout the country's municipalities.

Other pledges are coming from IBM with plans to train 150,000 people in cybersecurity over the next three years, Apple adding a new technology supply chain program and Amazon providing the public the same cybersecurity awareness training it gives to its own employees.

Big government or big brother?

Considering the massive cyber-attacks like those against SolarWinds, Colonial Pipelines, and most recently, Microsoft, and its massive record-breaking DDoS attack, it's no wonder that Biden's administration isn't just asking for help, it's demanding change.

Already this year, the Biden administration has swiftly signed the dotted line on three landmark reforms, demanding wide-sweeping changes in the cybersecurity landscape. These include:

- **Executive Order 14028, *Improving the Nation's Cybersecurity*[1]**
- **TSA Security Directive, *Pipeline-2021-01*[2]**
- **K-12 Cybersecurity Act**

Now we've seen the effects of immature cybersecurity models on both the public and private sectors. So, is policy enough to improve the situation? Time will tell.

But rest assured; this is not just a U.S. problem. All around the globe, nations are stepping up their cybersecurity defenses. The European Union Agency for Cybersecurity, ENISA, is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe.

The agency has been further empowered by the EU Cybersecurity Act granting a permanent mandate to the agency and giving it more resources and new tasks.

Additionally, earlier this year, ENISA and CERT-EU announced the signature of a Memorandum of Understanding to start their structured cooperation of working in harmonious cooperation to achieve a high common level of cybersecurity across Europe.

In the Asia-Pacific (APAC) region, Japan introduced updates to its Act on the Protection of Personal Information (APPI), increasing the obligations of covered entities to be more transparent and secure with regards to the safeguarding of resident data or face severe financial and criminal penalties.

Other APAC countries are revisiting existing cybersecurity laws as well. For example, Australia is currently reviewing proposed reforms to the Privacy Act, including increasing penalties under the Act to: AU$10 million, three times the value of the benefit obtained through the misconduct, or 10% of annual turnover.[3]

Not to be outdone, by February 2022, Singapore's amendment to the Personal Data Protection Act of 2012 (No. 26 of 2012) will increase the non-compliance penalty to either up to 10% of an organization's annual turnover in Singapore, for those with annual turnover that exceeds SGD 10 million, or SGD 1 million, whichever is higher.[4]

[1] Federal Register : Improving the Nation's Cybersecurity

[2] ________

[3] https://www.dlapiperdataprotection.com/index.html?t=enforcement&c=AU

[4] https://www.dlapiperdataprotection.com/index.html?t=enforcement&c=SG

Risk responsibility by mandate

All of these are welcomed announcements, but suggests the question of **who owns cybersecurity risks** to our nation, state and local governments, private sectors, and individual organizations?

As big government is now teaming up with big tech, it may seem easy to default to it being a combined effort, and we might have the same belief that it's a combined approach for our own companies.

However, with growing state and federal regulations, it may not be that simple.

Consider the State of New York's Department of Financial Services 23NYCRR Part 500 or simply NYDFS Part 500, for short. It is a regulation establishing cybersecurity requirements for financial services companies operating within the state.

When it went into effect on March 1, 2017, New York became the first state in the country to have a regulation requiring that any covered entity "shall designate a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy", per part 500.4 Chief information security officer.

The key term in the language of the regulation is "qualified individual", specifically the CISO of the company, or that of an affiliate or third-party. To avoid deflection of responsibility, the regulation also requires that a high-level senior member of the covered entity oversee the program in the case of the latter two options.

This now means one way or another, a named individual from the company is going on record as being the person responsible for the organization's cybersecurity program and compliance with all the requirements of NYDFS Part 500. If New York is acting as the bellwether, this type of legislation could be coming to a state or country near you.

Fast-forward to 2021 and look at the fallout that occurred because of the Colonial Pipeline cyberattack. It was the largest cyberattack on an oil infrastructure target in the history of the United States, causing massive six-day disruption of fuel distribution along the company's pipeline which serves most of the southeast region and extending as far north as New York.

In response to the incident, on May 28th, 2021, the Transportation Security Administration (TSA) issued its first of two new mandatory cybersecurity directives for the owners and operators of pipelines in the United States.

This ground-breaking directive now making compliance mandatory (rather than recommended, as in years past) places three requirements on all those owning and/or operating U.S. pipelines:

1. All cybersecurity-related incidents must be immediately reported to the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) within 12 hours of discovery and backed up by a $7,000 per day fine for non-compliance.
2. Designate a primary and alternative Cybersecurity Coordinator, at the corporate level, who is accessible 24/7 to TSA and CISA, and
3. Conduct a cybersecurity vulnerability assessment and provide a report of this assessment to TSA and CISA within 30 days of the directive, along with a gap remediation plan.

The second directive issued was not released publicly due to its sensitive nature, but what's known about it is the immediate demand for pipeline companies to beef up cyberattack mitigations, develop operational contingency and recovery plans and conduct cyber architectural design reviews. This directive has teeth. Failure to comply could mean financial penalties as high as $11,904 per violation, per day of non-compliance.

How will this affect you?

As state and federal regulations continue to mount and grow in complexity, it is expected that new roles will be developed to support and ensure compliance with these regulations.

Furthermore, we expect to see a branching off from the traditional IT/SecOps organizational chart into cyber risk roles that do not report to the same structure. Such titles may include Cybersecurity Risk Officer, Incident Risk Manager, and VP of Cyber Risk & Compliance with accountability to Legal departments in most cases and directly to Board of Directors in others.

Policy enforcement pushes down; accountability and reporting pushes up.

Average end-user impact

For the average end-user, the direct impact will likely result in new device and data policies being pushed by group policy and/or mobile device management (MDM) platforms. Additionally, users will be required to classify document types, sensitivity labels, and use FIDO2-compliant secured logins for two-factor authentication.

IT/SecOps changes

For the IT/SecOps admins, they can expect to see infrastructure changes necessary to add protective controls such as those to support the end-user security mentioned above, and also controls to support the general confidentially, integrity and availability (CIA) triad of our networks, servers, data, devices, and identities.

Accountability

Combining these administrative and technical controls, those responsible for organizational cybersecurity risk management programs will have the necessary data points to be able to detect, respond, and report cyber incidents as they occur, to remain compliant with the demanding timeframes set forth by regulatory authorities.

What's next?

Now, at the federal level, pressures are mounting for private sector companies falling under the regulations to provide stronger cybersecurity controls, report incidents at breakneck speeds and, place a head on the chopping block for non-compliance.

So as more and more states and federal agencies apply even greater pressure and ask the question "who is responsible for your company's cybersecurity risk management program?" will you know how to respond?

When surveyed, here is where on the corporate org chart our respondents landed on the question:

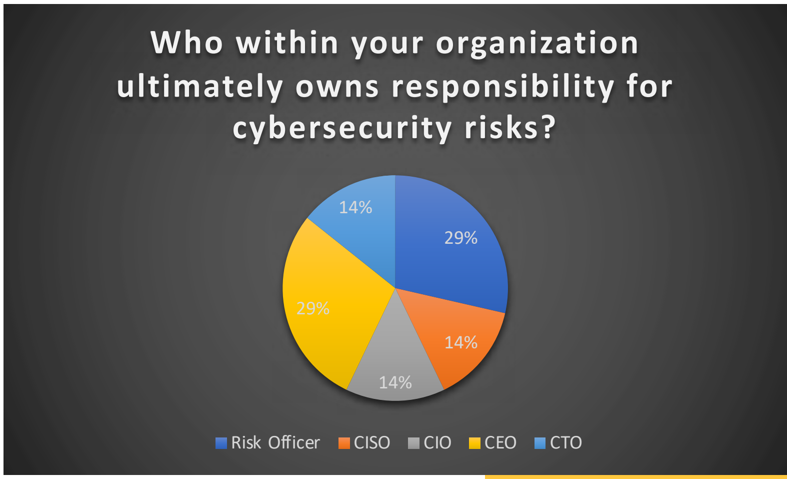


Figure 2 - Online survey results, Aug. 2021

It goes without saying that companies today are facing greater cybersecurity challenges than ever before, and mitigating the risks associated with an infrastructure breach or a resulting data breach can be devastating to the bottom line. But now we also must ask ourselves, what is the intention behind all of this?

What will, say, New York or the DHS/TSA do with the information being collected about our company executives? Could these individuals become subject to personal penalties or become subject to civil litigation? Time will tell, but nobody can argue the need for greater protections against the malicious actors out there that intend to do us harm and profit from the misdeeds.

How Exabeam can help reduce your risk exposure:

Traditional security tools, with rules and signatures-based controls, can't adapt to the new world of cyber threats. To keep up with the growing number of daily threats, understaffed security teams need next-gen, cloud-delivered solutions and tactics focused on generating outcomes, consistently and repeatedly.

Exabeam reduces your operational risks with a foundation built on behavioral analytics for users and entities, automation, and playbooks to help you make the next right action and use case content that aligns with the MITRE ATT&CK® framework.

These Threat Detection, Investigation & Response (TDIR) use case content packages address the complete lifecycle of SecOps workflows that includes prescribed data sources, detection models, watchlists, investigation checklists and response playbooks to help analysts deliver consistent, informed outcomes.

Get the fast track on insider threats

Manage insider threats that were previously difficult or impossible to detect. Behavioral analytics allows analysts to reliably distinguish the activity of attackers, or malicious insiders, from normal user or entity behavior—without generating false positives. Activity is then displayed in machine-built Smart Timelines, so analysts get visibility of an attacker's complete journey instead of a list of alerts.

Modernize your SOC

Cloud-based analytics and automation allow security teams to expand beyond traditional security information and event management (SIEM) use cases and improve their capabilities. With behavioral analytics, they can detect attacker tactics and techniques directly instead of relying solely on alert-fatigue generating threat intelligence libraries. Automation helps improve productivity at every phase of their workflow, from collection through investigation and response, and reduces time to resolve incidents.

Maximize your protection with the leading Next-Gen SIEM and XDR

The reality of today is we are dealing with highly trained and committed adversaries. The headlines don't lie, attacks are on the rise, and their one thing in common is the use of valid user or entity credentials.

These adversaries are hidden in plain sight, masquerading as legitimate users or devices. Understanding the data, behavior and identity of our users and assets is a critical requirement for any SIEM or XDR.

Behavioral analytics, the context they deliver, combined with automation, are often your only defense to help you stay out of the headlines.

See our products in action

Experience the benefits our customers see today

Get a Demo >

- No more blind spots – collect and analyze unlimited log data
- Detection of advanced cyber threats, which traditional tech can't see
- Dramatically reduced investigation timeframes via our Smart Timelines
- Efficient response with playbook-based automation

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. The leader in next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. Exabeam offers a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. We design and build products to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives and best protect their organizations.

exabeam

For more information, visit

TUCANA
CYBER SECURITY SOLUTIONS
www.tucana.com info@tucana.com