Chief Information Security Officer QuickStart PLAYBOOK

Chief Information Security Officer QuickStart PLAYBOOK

1. PREPARE

Know the "Risks" … all of them—the company's, your clients, the public, partners—even your own!

Identify your Champions … Who's on your "team" doesn't always mean those who are assigned to work for or with you. Who in the organization supports why you're there?

2. ACT

Classify the Assets … What does the company consider its commodity (beyond its employees—what generates revenue)?

Evaluate the Current Posture … Does the company have a current Security Process defined? What controls does it deploy? Where are the gaps?

Build your Plan of Attack … Prioritize your time, tools & people, and create 30-, 60- and 90-day Benchmarks to achieve and manage expectations.

3. REVIEW

Document What Works … Make sure those short-term successes are identified (and passed along to recognize those within your team—away from yourself!).

4. REPORT

Deliver the Results … Just because "that's the way we used to do it" worked before—things change and so do the challenges with staying secure.

Chief Information Security Officer QuickStart PLAYBOOK

Don't shoot the messenger!
Almost immediately upon taking the job, cybersecurity leaders face a range of challenges as they tackle the challenges to establish an effective defense around their company's protected assets.

WHY DO YOU NEED THIS?

The Digital World is seeing more and more companies with executives who are not prepared to do what is needed to keep their assets, products or services secure.

There's no "Magic Bullet," but these seven steps can help new CISOs take on the challenges they will be most likely to face in their first 90 days on the job.

Following a post-pandemic, the shift to a remote workforce, the uncertainty of what needs to happen, the order and priority of how to manage risk, and who to call when the trouble happens, often falls on resources that may not be fully prepared for navigating the challenges that follow.

Whether you are a seasoned CISO or a freshly minted cyber-professional, as you adapt and improve your risk defenses, Drew Blandford-Williams brings close to five decades of experience in helping you plan, develop, maintain and improve your cybersecurity posture.

If you're stepping into the role and want some reassurances that you're doing it right—whether you are conducting interviews, workshops, tabletops or writing those volumes of policies, procedures and framework support plans, don't go it alone!

This QuickStart Playbook can keep you on track.

Let's Do This !

PHASE 1a

KNOW THE RISKS

Know why you're here!

At the core of your role as CISO is managing risk throughout the organization. Knowing which risks are likely to impact your business doesn't mean everything all at once—you need to know how and where your business operates, allowing you to identify the most relevant risks.

Here are the five key areas for you to investigate starting on Day One:

1. **Environmental** risks
2. **Gaps** in controls
3. **History** of security incidents
4. **Compromises** to data privacy
5. **Compliance** concerns

Risk Assessments are required by most of the national and international compliance regulations. If HIPAA, PCI, GDPR, CCPA, or the intensive SOC2 audit is on your horizon, then an information security risk assessment is a must-have for your organization.

Avoid Wearing the "KICK ME!" Sign

When / if problems surface (relating to cybersecurity), they may fall to you to address, but a bad situation and the message of what needs to happen to fix it are not tied to you *(but it happens!)*

To build confidence and [maybe?] stir up the operation to increase awareness—preparing a Baseline Infrastructure Risk Assessment ("BISRA") should be one of the first plans you make to execute (or review—if the organization has had one in the past year).

Preparing a BISRA will help you assess the general threat landscape within your organization and identify vulnerabilities in information systems and help you and your team determine the likelihood of a potentially compromising event will occur, and aid in your decision-making on where to focus your time, resources and any potential funding needs.

Be sure to consult with staff members—you're trying to raise awareness for how to better defend against a compromise to the confidentiality, integrity and availability of your business.

And making a few friends won't hurt either ☺

PHASE 1b

IDENTIFY YOUR CHAMPIONS

Who in the organization supports why you're on the team, and how can YOU help Them?

Pick a Winner! For change of any real substance to occur, a sense of urgency must be created.

This urgency might occur due to actions imposed upon an organization by outside forces (a ransomware attack, etc.), or it may occur because of some self-imposed action, such as a new GRC mandate.

The Champion's role, whether out of a response to an incident or as part of the day-to-day operations, means driving the business to improve, even when internal interests (and company politics) may resist.

Team Champions are often assigned tasks after-the-fact and feel a greater sense of urgency. Getting the team to share a common sense of urgency becomes the first challenge, and often requires you as the "New Guy" to work from the inside out (rather than trying to introduce an external process or resource that may be seen as threatening).

☆ ADAPT OF DIE! ☆

Since the beginning of the Digital Age, organizations have had to face the task of learning how to adapt to change

Within your first 90 days, consider the following five steps in helping you establish the groundwork for how your organization (and its clients).

1. **Identify & Nurture a Pool of Champions** *(i.e., "Change Agents")*
2. **Establish Operational Urgency** *(a disruptive event might do this for you)*
3. **Form Coalitions of Support** *(Help break down the silo effect)*
4. **Create a Mission-critical Vision** *(You can't do business if you're offline!)*
5. **Reinforce Effective Communication Habits** *(How do communicate what is needed?)*

An effective CISO enlists champions who help define and improve the organization's risk appetite, threat landscape and cybersecurity policy.

PHASE 2a

CLASSIFY THE ASSETS

Asset classification means identifying the value of each asset and prioritizing how to secure it

How do you know what's important to your organization? Classifying your company's assets requires knowing first, what the company hods as its "Crown Jewels" and then assigning those assets to designated groups, based on six key elements:

- **Asset name**
- **Asset location**
- **Asset cost**
- **Asset owner**
- **Asset classification**
- **Data protection level required**

Once you have these six elements documented, it's time to manage, classify and designate appropriate security processes and controls around those assets. Take these five steps to making your determination:

1. **Create an asset inventory.**
2. **Assign ownership.**
3. **Classify based on value.**
4. **Protect based on classification.**
5. **Assess & review.**

"What's in YOUR Business?"

When classifying your organization's assets, you must take into consideration the three principles of Information Security: Confidentiality, Integrity & Availability.

What does your organization consider "Proprietary" vs "Confidential" (or both)?

Using the "Low-Medium-High" classification standard, as prescribed by the Center for Internet Security (CIS), you can begin to cross-reference each identified asset and determine its impact on the CIA Triad

1. What is the impact of unauthorized disclosure regarding:

    - **Data Privacy**
    - **Health and Safety**
    - **Financial Loss**
    - **SE Mission/Programs**
    - **Public Trust**

2. Which compliance-based mandates are impacted by the asset (which may also cause additional impact to your clients, partners or suppliers):

    - **PCI**
    - **HIPAA**
    - **NERC**
    - **FISMA**
    - **SOC2**
    - **Others?**

PHASE 2b

EVALUATE THE CURRENT POSTURE

You can't fix problems you don't know about

Cybersecurity Posture refers to the ability to respond to a security incident or event. A cyber event, while potentially devastating, can be studied—even planned for (to an extent), but success in addressing the appropriate response to a cyber event depends on the organization's current "Risk Posture" and its ability to respond and recover.

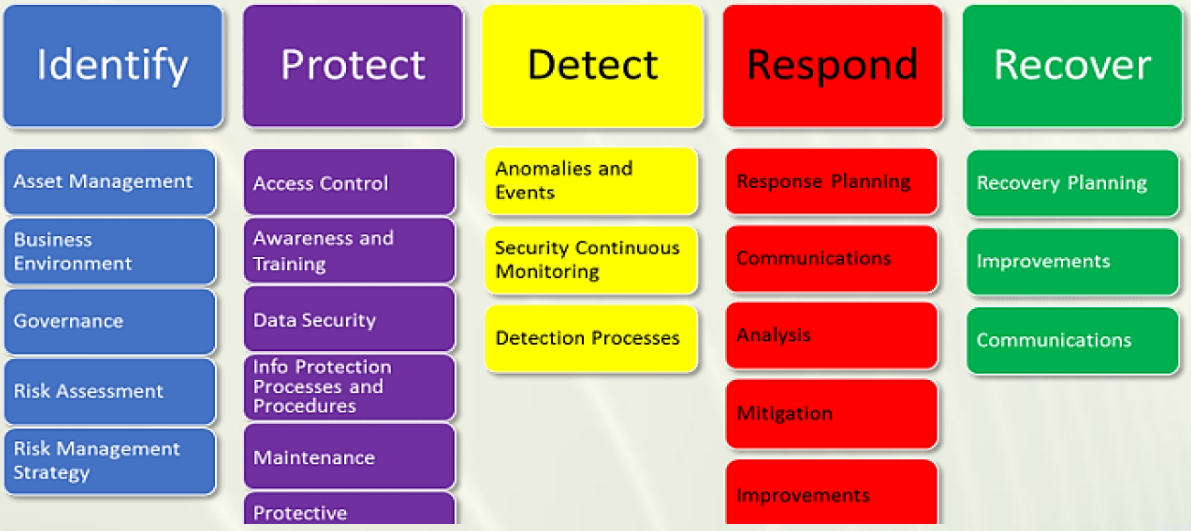
Understand what's at stake
and what matters to your organization

Information Security is one of the top concerns for business owners today.

As with any type of emergency event, cyber incidents may result in long-term consequences to an organization, its people and those whom it serves. The National Institute of Standards and Technology, established the NIST Cybersecurity Framework to help organizations of all sizes and disciplines in their respective efforts to manage risk and defend their operations from disruptive activities.

When looking at your business' "Threat Posture," the NIST-CSF is a good place to prepare your foundation for risk management evaluation, defense and remediation.

NIST RISK MANAGEMENT FRAMEWORK



PHASE 2C

BUILD YOUR PLAN OF ATTACK

Without planning, responding to an incident may be TOO LATE!

Every Business faces "Risk." Hackers constantly try to exploit vulnerabilities to steal key data, disrupt operations, and erode organizational credibility.

Regulatory and industry requirements require comprehensive security programs that protect customer information, with the consequences of heavy fines, should those procedures not be verified ("compliance") on a regular basis.

Threat actors are well-organized and often tied to state-funded organizations, with the objective of gaining access to sensitive assets and holding those assets hostage for millions of dollars.

But "Fear" doesn't fix problems, and planning and preparation can offer a proven defense plan, which is essential to helping an organization out-run the bad guys.

☆ Preparation is key ☆

Attacking a cyber problem should begin with anticipating how it will end

That may sound odd, but one of the first priorities you should consider in your role as CISO is establishing a comprehensive Incident Response and Business Continuity process.

When preparing your organization for the potential (or inevitable) cyber incident, ask your leadership the following questions *(and be prepared to get uncomfortable responses)*:

- Where do we believe is the greatest threat to our business?
- What are the tools we have currently deployed to defend our infrastructure, and who manages them?
- Do we have a system back-up plan, and if so, how often do we review it?
- What types of disruptive events are we likely to face and how prepared are we for these types of events?
- How does Leadership determine where to focus its attention, with respect to Cybersecurity?
- When can we set up an in-house exercise to review and test our awareness and response plans?

PHASE 3

DOCUMENT WHAT WORKS

If you find a process that works, document it and use it as a benchmark

Documenting your activities and those successes your team achieves along the way, provides you not only with good benchmarking data, it also provides you with a standard of practice to use that others can template for their own goals—the whole company wins!

Write it down

Documentation has become a mission-critical part of the role of the CISO. Your organization needs to take the idea of "Security" seriously, and someone once said, if you don't write down your plans and objectives, they remain part of your imagination, there is no standard established, and nothing is achieved.

When you're looking at those essential first 90 days to make a strong positive impact on the business, making sure that written policies, procedures, guidelines and operational parameters become the roadmap to achieving a greater level of success, as well as meeting those essential compliance requirements prescribed by all of the major mandates.

Here's your Documentation Checklist

(…the first things you should ensure your company has in place)

NIST / ISO27K ISMS	**Includes critical direction on key issues (password format, patch deployment timelines, multi-factor authentication, use of mobile devices, data back-up & retention, etc.)**
Business Continuity Plan	**One of the most important (and often overlooked), documents within any operation. The BCP establishes protocols for how to recover systems in an emergency.**
Risk Register	**Ensures the organization has appropriate risk management processes current and appropriate for their operations.**
Risk Awareness Plan	**This plan is a documented schedule for training, supported visual aids and other means of ensuring everyone in the organization is made aware (on a regular basis), of how to stay risk-averse in their daily work responsibilities.**

PHASE 4

DELIVER THE RESULTS

It's about building progress, based on adaptable, scalable and acceptable processes

Your role as a CISO gives you the opportunity to help shape the way the organization thinks learns, thinks and improves on its risk posture and cybersecurity defense tactics.

As you document what works and log the "small wins" that you and your team achieve, reporting on that progress provides peace of mind to other leaders, the staff and your organization's clients and partners.

Keeping the stakeholders apprised of your progress (and everyone is a stakeholder), helps remove the often-implied "mystique" that surrounds, not only your role, but the idea of what "Cybersecurity" is all about.

Your KPI's will likely be based on how well you perform without being noticed

Review & Revise: PROCESSES

As CISO, you are responsible for associated policies and procedures ("GRC"), as they apply to relevant mandates and standards (PCI, GDPR, HIPAA, SOC2, etc.). Reviewing those processes that your organization has in place, or is lacking, provides you with an immediate analysis of what has or has not been implemented, and what may be needed to achieve a baseline level of risk management.

Review & Revise: PEOPLE

No. You're not going to morph into the head of Human Resources! However, making sure your HR leadership understands what is needed beyond the standard background check—such as access control (based on roles), security awareness training, and onboarding/offboarding protocols—will have immediate impact on reducing the potential for *Insider compromises*.

Review & Revise: CONTROLS

Although there is often a desire by tech-savvy CISOs to begin campaigning for more money to spend on more controls, if you want to make a difference in those first critical days on the job, take an inventory of the tools the company already has, make sure they're the right tools for the job, they're properly deployed, managed and updated, and then determine what else (if anything) may be needed.

Good controls are only good if they are needed and work the way they're designed

About the Author

Drew Blandford-Williams

Drew Blandford-Williams began his career in Information Security while Jimmy Carter was still president. Drew launched one of the first Host Intrusion Detection systems (AXENT's Intruder Alert) and was product manager for one of the first SIEM tools (Enterprise Security Manager). He co-developed an early Security Services/Hacker Research team (Symantec SWAT) and was on the original team that transitioned the former Kennedy Kassebaum Act into what became the Health Insurance Portability and Accountability Act (HIPAA). Drew was also part of the core development team, working with MITRE to establish the CVE reference system for all reported hacks and vulnerabilities.

He has presented to the UN Security Council on Information Warfare, has written hundreds of cybersecurity GRC policies for organizations spanning all 16 critical infrastructures, and Drew's knowledge and experience with NIST and ISO cybersecurity frameworks comprise his background in writing training manuals, delivering tabletop exercises and ransomware defense tutorials.

Drew has a master's degree in Homeland Security Leadership from the George Washington University and an undergraduate in Technical Communications from Brigham Young University.

A former university faculty member, contributor to CSO Online, featured resource on the Wall Street Journal, Washington Post, USA Today, and MSNBC, and former host of Hacker Halted Asia, Drew was also the first principal funding source for the Black Hat Briefings.

And he takes the subject of "securing everyone for a safer world" to heart.

"Information security management is an evolved process. You have to love solving problems —even when those around you find it a challenge to solve those problems."