What the world of sports teaches us about incident preparedness and response

Jun 22, 2021 Save This ()

Anderson Lunsford
IAPP Member Contributor (/about/person/0011a00000DlCglAAF)

Alexandra Ross, CIPP/E, CIPP/US, CIPM, CIPT, FIP, PLS
IAPP Member Contributor

Privacy and security incidents have become ubiquitous across organizations of all sizes and sectors. According to Verizon's most recent (https://enterprise.verizon.com/resources/reports/dbir/) Data Breach Investigations Report, data breach volume doubled from 2018 to 2019. Whether an organization operates in the financial services sector or the manufacturing industry, the importance of preparing for these inevitable events is well understood. However, knowing what constitutes best practice for incident preparedness is not fully appreciated, even though implementing those practices benefits companies beyond regulatory compliance.

The technical complexity of cybersecurity and the legal complexity of data breach obligations often leave many feeling too overwhelmed to devote adequate time to preparation. In reality, the elements of a good incident response program are straightforward, mirroring the patterns of success seen in other disciplines, including how sports teams prepare, adjust to change and leverage new technology.

The best teams prepare with thorough game planning and actionable playbooks

Across all sports, the best teams, coaches and players consistently take preparation just as seriously as the game itself. A strong common denominator why the best coaches and players consistently succeed is because they prepare more than their competition. They build game plans and playbooks that play to their strengths and capitalize on the competition's weaknesses. They go into every game with a clear strategy of what it will take to win, and that strategy includes utilizing detailed plays designed for every situation they think they might face during the game.

they think they are likely to face.

When organizations begin creating an incident response program, they usually start with a high-level plan or checklist that centers around immediate triage activities. For example, such plans may include a list of who to contact, incorporating the internal team (including security, legal and operations), outside counsel, forensic consultants, cyber insurance firms and other relevant groups. However, when those organizations experience real-time incidents, it can quickly become apparent that such high-level plans don't provide any guidance on the actual work that needs to be done.

Imagine if a team put together a starting lineup and just planned to "'figure it out'" once the game started. Even if the team was stacked with the all-star players at every position, it would quickly be blown out by the other team. In the same way, having the best law firm and forensic consulting firm on retainer won't guarantee the response to the incident will go well — most likely, it will just guarantee it will be the most expensive.

Ultimately, there is no "one-size-fits-all" incident response plan. Instead, the best incident response plans are made up of multiple case-specific playbooks developed for each type or category of incident. Using a modular approach like this ensures the correct sequence of response tasks can be rapidly identified in the event of a specific incident or breach.

Game plans and playbooks must be dynamic

Inevitably once a game begins, playbooks and strategies must be adjusted. In fact, the TV interviews with coaches at halftime always revolve around what adjustments the coach thinks the team needs to make in the second half. The best coaches and teams are adept at making key adjustments because they employ adaptive strategies when forced to execute on the fly outside their playbooks. In contrast, if a coach or team had a static game plan that was rarely updated, it is unlikely the coach and team would be successful.

Similarly, putting together an incident response plan in static documents and spreadsheets is likely going to leave an organization reeling in the way boxer Mike Tyson famously said, "Everyone has a plan until they get punched in the mouth."

In incident response planning, a static and manual approach very quickly becomes ineffective when put to the test.

For example, there are many free, purportedly comprehensive lists on the internet of all data privacy regulations. In addition, some law firms offer quarterly updated spreadsheets containing the most recent iteration of data privacy requirements across jurisdictions worldwide. Some organizations may falsely think this type of subscription suffices for being prepared. However, as soon as an incident occurs, these compendiums of requirements have little to no value because they may no longer be current and are unlikely to be tailored to the organization and circumstances at hand. As a result, these lists will be quickly thrown aside, and the organization must then spend valuable time figuring out what it must do to respond.

Figuring out what to do includes:

- Determining the business impact of temporarily shutting down systems and services for your customers, partners and employees.

brand damage and simultaneously avoids additional liability.

- Running a state, country and/or worldwide analysis of which regulations apply to the given event.
- Examining hundreds to possibly thousands of contracts that might apply to the circumstances.

These activities lead to determining what actions need to be taken. Meanwhile the shot clocks for breach notification have already started ticking, from 72 hours in the case of the EU General Data Protection Regulation to as short as 24 hours or less in other jurisdictions or from common notification terms in contractual agreements. Simply put, relying on a checklist for incident response is not sufficient because of the speed and efficiency demanded in the process. Companies must take a more proactive and dynamic approach to meet these deadlines.

Elite teams embrace and leverage new technology whenever possible

The evolution of applying new technology to sports continues to pick up pace in the same way it does in the business world, and elite sports teams invest heavily in tech to leverage any advantage it can provide. For instance, golf club manufacturers develop new clubs every year, adding valuable distance to drivers and ball control with irons. In American football, quarterbacks utilize virtual reality headsets to practice reading defensive coverage. Even coaches perceived as “old school” understand that failing to adapt at least in part to new tech will be detrimental to their teams.

The best incident response programs have similarly embraced new tech. Workflow automation software can make the incident response process exponentially faster and less stressful while simultaneously more reliable. Instead of doing a state-by-state or country-by-country analysis every time your organization has an incident, tech with privacy and other relevant regulations baked in can be leveraged to eliminate that time-consuming part of the process.

Using software, an incident response team can input the elements they know about an incident and immediately know which regulations apply and the tasks that need to be completed to meet those requirements. Similarly, the software can utilize the data input to automatically generate the analysis and actionable tasks needed to meet contractual and policy requirements. With all requirements accounted for and all the necessary tasks to meet those requirements provided, an organization moves from finding out about an incident to immediately executing a response — minimizing precious hours and days otherwise spent figuring out what needs to be done.

In addition, by leveraging an incident response software platform to centralize all data breach response plans and related information in a single place, stakeholders and incident response teams can collaborate, carry out their assigned tasks and document their actions taken quicker. Then if an audit, investigation or litigation occurs after the incident, the timeline of events is ready to prove the company handled the incident properly.

taken in the response effort. This type of system takes a lot of manual effort and often leads to factual inconsistencies because there is no single source of truth the team can rely upon during the incident or after the incident response is complete. Bringing it back to sports, using spreadsheets or documents to record response activities is like relying on handwritten notes to review the plays of a game in lieu of relying on video recordings.

Proactive readiness is the path to victory

Data breaches and privacy incidents are recurring issues facing all organizations. The best incident response programs will view incident response as regular enterprise workflow and not a singular or siloed activity. Just like in sports, if companies proactively prepare, practice, evolve and use technology, they can make the management of breaches and incidents more routine. Managing incidents routinely rather than as a crisis makes organizations more resilient and mitigates the potential fallout for a mishandled event. Ultimately, a sophisticated incident response program reduces risk, enhances customer loyalty and builds brand trust.

Pease International Tradeport, 75 Rochester Ave.
Portsmouth, NH 03801 USA • +1 603.427.9200