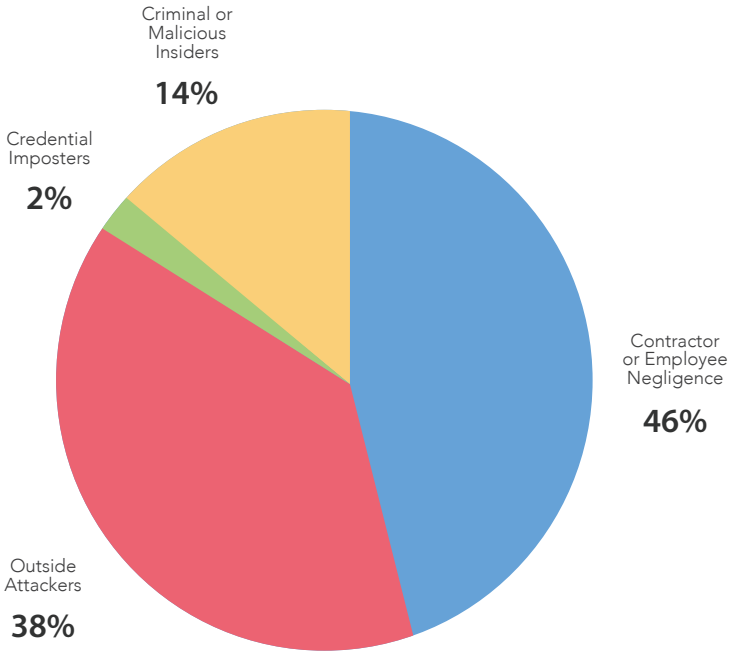
Veriato

# Effective Incident Response Through User Activity Monitoring

**By Derek A. Smith** (CISSP)

www.veriato.com




Cyber attacks, data breaches, and the disruptions they bring are considered a fact of life by the majority of Americans [i]. Nearly 65% of Americans have personal experience with the collateral damage [ii] of a data breach, and more than three-quarters of American adults are aware of at least one high-profile data breach in the private sector.[iii]

According to recent reports [iv] [v], 60% of all cyber incidents are caused by "insiders," that is, employees, contractors, and others granted access credentials by the organization. Moreover, 56% of occurrences are purposefully initiated with criminal or malicious intent.

The result is that the average organization experiences 23 significant, asset-threatening cyber incidents per year. Furthermore, there is a 26% probability that one or more of these incidents will result in a material data loss.

With the cost of a data breach eclipsing the $4 million mark,[vi] organizations need to pay close attention to any suspected cyber incident.

## TIME IS THE MOST IMPORTANT CYBER INCIDENT FACTOR

The time to compromise an IT system is often measured in minutes.[vii] If bots or other scaled automation is involved, that time may be pushed down to mere seconds. If the compromise results in data exfiltration, for days the company may be hemorrhaging confidential consumer information, trade secrets, pre-publication financials, strategic plans, employee social security numbers, or whatever else the attackers want.

The very sobering reality-check is that, on average, the time to discover a compromise to the IT security system is measured in – not minutes, not even in days, but in months and sometimes in years. Moreover, the time it takes to contain the incident – specifically, the time to root out the discovered compromise from the IT system – is measured in days and weeks. The longer a cyber incident remains undiscovered, the more likely it will be that the company will realize a significant data breach. Such incidents cost the company millions in lost business, lost opportunities, tarnished reputation, and lawsuits. These costs are in addition to that of the lost or compromised digital assets and the direct incident containment costs.

# CHALLENGES TO INCIDENT RESPONSE

The top five challenges to responding to suspected cyber incidents [viii] – especially from sophisticated attackers – all have a critical time element. Moreover, the longer it takes to respond, the more costly an incident may become. The top five challenges include:

1. **Correctly identify an actual "incident" from background "noise."** Traditional cybersecurity monitoring systems have great difficulty correctly differentiating between an actual incident which needs a response and the plethora of background security "noise." This is why incidents – especially those caused by insiders and misuse of account privileges – can take months, even years, before discovery.

2. **Analyze all relevant incident data to determine what happened and what the intention (if any) of the actor/s**. Often the only computer logs available to the forensic investigation team are from firewalls or other technologies whose principle function is to mitigate outside attackers. Such records will contain little to no information regarding events that occurred after the actor(s) pass security.

3. **Identify what was compromised in the system, the network, and the digital assets**. Every CEO is concerned about the company experiencing a "reportable event" – that is, one in which confidential customer data was breached. However, many non-reportable events may be even more damaging or costly to the organization. For example, loss of company confidential data (i.e. strategic marketing plans or employee records) or a compromise of system functionality (which could make it possible for hackers to spoof banks into transferring millions of dollars into the hacker's accounts). Understanding what may have been compromised is crucial to determining the underlying intent or motive of the actor(s).

4. **Quantify the potential technological and business impact of the incident.** An important step in preparing an effective incident response strategy – one whose importance cannot be overestimated – is to quantify the technological and business impact of it. Naturally, thorough analysis can only be done if everything compromised during the incident is known. Furthermore, quantification of the technical impact is distinct from quantification of the business impact. There is no immediate, direct business impact, for example, with "sleeper" malware left behind – it is not doing anything. However, the technological impact of such malware may be catastrophic if it is activated before the security team can remove it.

5. **Conduct a thorough investigation.** Beyond understanding the "what" and "when" of an incident is gaining an in-depth understanding of the "who" and "why." Consider a hypothetical event in which malware is introduced to the system through an employee's computer. Security's first response may be to treat it as a criminal attack. However, a thorough investigation may reveal that the employee was simply unaware that setting his smartphone down next to his work computer allowed the phone to communicate with his work computer via an active Bluetooth connection. Not only was there no malicious or criminal intent, but the investigation, in this case, may be used during the company's next cyber security training on how employees can become unwitting "helpers" to outside attackers.

## Incidence Response Mistakes

Responding to identified cyber incidences promptly is the most important part of an incident response strategy. However, there are three things which an organization should avoid as part of their response:

1) **Pulling the Plug.** Computers operate on electrical power. Thus, if an attacker manages to get past the established defenses, the initial response may be to shut off the power rather than risk data exfiltration or other harmful attacker activity.

   However, while cutting the power may initially stop the attacker's current activity, the consequences of doing so will put the attacked organization in a worse position.

   Cutting the power will result in loss of information stored in volatile memory. That information will undoubtedly relate legitimate business activity and billable work in progress – which may be lost forever.

   Moreover, important forensic information will be stored in the volatile memory. Shutting down the power may actually help the attacker get away clean.

Promptness is key to incidence response. However, promptness at the cost of effectiveness is no win for the organization. Avoid these costly mistakes after identifying an incident:

2) **Losing the log Files.** The computer's logs of activity before, during, and after the identified event are invaluable when it comes to identifying the actor(s), the intent behind the incident, what containment is necessary, and what technological and business ramifications will need to be remediated.

   Furthermore, the logs will be key forensic evidence should the incident response result in criminal or civil prosecution. Having and keeping thorough, detailed incident logs is crucial to incidence response.

3) **Treating the incident Lightly.** Every incident – regardless of whether or not it resulted in a breach, was caused by simple neglect or nefarious motives, or was an insider or outsider event – is a learning experience for the organization. Each is a case-study in real-world incident response intelligence. Learn from it.

## How UAM Promotes Effective Incident Response

Veriato 360 monitoring technology helps organizations beat the incident response time-crunch at each of the five most challenging areas:

1. **Veriato 360's powerful activity alerting keeps you immediately informed about potential security and policy violations.** Traditional technologies leave security teams buried under a daily mountain of "possible" incidents. Often the first clue that an actual incident occurred is a public news report about breached data sold on the dark web. Recon's UBA capabilities, on the other hand, alerts security as soon as any suspicious activity is detected – long before a potential incident can develop into a realized system compromise.

2. **ALL user activity recorded and stored.** Whereas defensive technologies primarily log outsider infiltration attempts, 360 actively monitors and records every user's activity – down to the last keystroke – and stores that information in an obfuscated, encrypted file on the users' computer. Recorded data may be searched by keyword, user, date, or other indices, and can be easily reviewed via DVR-like playback. Security teams can quickly identify potential issues and understand the events and context of the identified incident.

3. **The dashboard allows security teams to identify activity patterns quickly.** The organization employing Veriato need never wonder "what happened" with Veriato's ability to search for multiple strings within specific activities or across all recorded logs. Also, the dashboard's capacity to look backward at events will help security teams identify significant things previously overlooked. For example, specific communication activities which were not initially deemed necessary to generate an alert on can be located quickly and efficiently.

4. **Having a detailed, user-by-user record of what happened provides the necessary forensic data to quantify the potential impact of an identified incident.** Veriato 360 can, for example, quickly alert HR and security when an outgoing sales person attempts to download the company's customer database – which could potentially be used by the individual to poach customers when he gets to his new position. The result of such a data theft would undoubtedly lead to a material loss of revenue for the company. Using the Veriato system, however, the organization not only would be notified that the outgoing sales person is thinking about the data theft but would provide a detailed record of the theft events.

5. **Conduct a thorough investigation.** Veriato provides the analytic and real-time data investigators need to conduct a thorough and timely investigation. The detailed record of all computer activity recorded by Veriato 360 allows investigators to zero in on the events that occurred quickly. Investigators can quickly and easily understand the "who," "what," "where," "when," and "why" of any incident and efficiently bring the incident investigation to an effective conclusion.

Veriato 360 is fast, detailed and easy to use. An IT team is not needed to utilize the software, saving an organization critical time and money. Veriato 360 makes the effective incident response a practical reality – every time.

[i] Olmstead, Kenneth and Aaron Smith. "Americans and Cybersecurity." Pew Research Center: Washington DC. January 26. 2017.
http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

[ii] Agarwal, Anurag (Archie). "Data Breaches and their Collateral Damage." Anurag (Archie Agarwal. LinkedIn.com: Mountain View. August 5, 2016.
https://www.linkedin.com/pulse/data-breaches-collateral-damage-anurag-archie-agarwal

[iii] Olmstead, Kenneth and Aaron Smith. "Attitudes about Cybersecurity Policy." Pew Research Center: Washington DC. January 26. 2017.
http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

[iv] "2016 Cost of Insider Threats." Ponemon Institute, LLC: Michigan. September 2016.
https://dtexsystems.com/cost-of-insider-threat/

[v] van Zadelhoff, Marc. "The Biggest Cybersecurity Threats are Inside Your Company." Harvard Business Review. Harvard University: Boston. September 19, 2016.
https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

[vi] "2016 Cost of Data Breach Study: Global Analysis." Ponemon Institute, LLC: Michigan. June 2016.
https://www-03.ibm.com/security/data-breach/

[vii] "2017 Data Breach Investigation Report." Verizon Enterprise: New York. 2017.
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[viii] "Cyber Incident Response Management." IT Governance: Ely, UK. 2017.
https://www.itgovernance.co.uk/cyber-incident-response-management

Veriato
www.veriato.com

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410

Veriato EMEA
3rd Floor, Steward House
14 Commercial Way
Woking, Surrey
GU21 6ET, United Kingdom

https://plus.google.com/+Spectorsoft
https://www.linkedin.com/company/veriato
https://twitter.com/Veriato
https://www.youtube.com/SpectorSoft
https://www.facebook.com/VeriatoInc/