THE ECONOMIC VALUE OF PREVENTION IN THE CYBERSECURITY LIFECYCLE

Study by Ponemon Institute
Sponsored by Deep Instinct, April 2020

SUMMARY

We worked with the Ponemon Institute to survey over 600 IT and security practitioners about their security stack and their perception of the effectiveness of prevention within the cybersecurity lifecycle.

THE KEY TAKEAWAY FROM THIS RESEARCH ARE

- While 70% agree that the **ability to prevent cyberattacks would strengthen their cybersecurity posture,** most (76%) say that **they focus on the detection and containment of cyberattacks because prevention is perceived to be too difficult to achieve.**

- **Organizations are most effective in containing cyberattacks.** 55% say their organizations are highly effective at containing attacks in the cybersecurity lifecycle. Less than half (46%) say their organizations are effective in preventing cyberattacks. 80% say prevention of a cyberattack is the most difficult to achieve in the cybersecurity lifecycle, this is followed by the recovery phase at 79%.

- **Organizations are making investments in technology that do not strengthen their cybersecurity posture as they're based on the wrong metrics.** 50% say their organizations are wasting limited budgets on investments that don't improve their cybersecurity posture.

- The average total IT budget is $94.3 million, with 14% or approximately $13 million allocated to IT security. 19% or roughly $2.5 million for investments in enabling security technologies such as AI, machine learning, orchestration, automation, blockchain, and more.

- 67% believe the **use of automation and advanced AI would improve their ability to prevent.**

Prevention of attacks can reduce the cost of an attack significantly. To determine the **economic value of prevention,** respondents were first asked to estimate the cost of one of the following five types of attacks: phishing, zero-day, spyware, nation-state and ransomware. They were then asked to estimate what percentage of the cost is spent on each phase of the cybersecurity lifecycle, including prevention.

KEY STATISTICS

The findings include the approximate cost savings that can be gained from effective prevention:

- **91%** of costs eliminated in a nation-state attack, resulting in an average cost saving of **$1,366,365**
- **88%** of costs eliminated in a zero-day attack, resulting in an average cost saving of **$1,089,440**
- **90%** of costs eliminated in a ransomware attack, resulting in an average cost saving of **$396,675**
- **82%** of cost eliminated in phishing attack, resulting in an average cost saving of **$682,650**

For example, the average total cost of a phishing attack is $832,500, and of that, detection, containment, recovery, and remediation represent 82% of the total cost. Respondents estimate spending 18% on prevention (this includes ongoing infrastructure and security maintenance). Thus, preventing an attack can save $682,650 (82% of $832,500).

Download the **full Report**