What's the risk?

A cyberattack can have devastating effects for the victims. In 2017, victims of cybercrimes lost over $1.4 billion.4

The cybersecurity team at Georgia State University started noticing a steady uptick in malware attacks, particularly phishing. 8 They deployed Advanced Threat Protection to a pilot group and saw a reduction in the number of emails that got through with malicious content by more than 2,000 messages over a five-month period.9

Join the hunt to find cybercriminals

In September of 2018, the FBI issued an announcement that schools need to take a larger role in protecting the personal information of K-12 students across the country.10 The FBI has been working to educate higher-education business decision makers on their role in thwarting cyberthreats since 2011. 11

Consider these specific cases

A malware attack involving an e-mail containing the Emotet virus at a North Carolina public school cost that district $314,000.5 Every county server was affected, and it took weeks to recover data from backups, some of which were also affected by the malware. This malware attack encrypted critical files and sent the school a ransom note with instructions to pay the bad actors in bitcoin, claiming to send a key to recover the files in exchange for payment.

Another public school in Bingham County, Idaho suffered a network system outage for six weeks after a ransomware attack. 6

What can you do?

In the higher-education space, Iranian bad actors targeted over 140 US universities and over 8,000 individual accounts, stealing more than 31TB of information, amounting to more than $3 billion in intellectual property.7 The defendants in that case are still fugitives from justice.

The attack risks with the greatest frequency are: advanced malware, advanced persistent threats, DNS-based data exfiltration, unauthorized network access, phishing and social engineering.8 The most popular cyberattacks occur via e-mail,3 because of the easy access to accounts, as well as the visibility of e-mail.

Understanding cyberattack characteristics is the first line of defense in saving an educational institution the time, effort, and costs associated with recovery.

In the past, it was difficult to get an institution's cybersecurity health under control. Now, it’s easier than ever to help protect against cyberattacks.

Register for a security briefing ›
Contact us directly to talk about your security strategy ›

Get ahead of the problem

In the higher-education space, Iranian bad actors targeted over 140 US universities and over 8,000 individual accounts, stealing more than 31TB of information, amounting to more than $3 billion in intellectual property.7 The defendants in that case are still fugitives from justice.

The FBI has been working to educate higher-education business decision makers on their role in thwarting cyberthreats since 2011. 11

School administrators and IT staff can take back their power and get active in the fight against cybercrime.

In September of 2018, the FBI issued an announcement that schools need to take a larger role in protecting the personal information of K-12 students across the country.

Join the hunt to find cybercriminals

The FBI has been working to educate higher-education business decision makers on their role in thwarting cyberthreats since 2011.11

School administrators and IT staff can take back their power and get active in the fight against cybercrime.

In the past, it was difficult to get an institution’s cybersecurity health under control. Now, it’s easier than ever to help protect against cyberattacks.